UNIVERSITÉ DE LORRAINE

École doctorale IAEM Lorraine

Approches Graphiques en Informatique Quantique

THÈSE

pour l'obtention d'une

Habilitation de l'Université de Lorraine
(mention informatique, CNU section 27)

par

Simon Perdrix

Soutenue le 19 septembre 2019

Composition du jury :

Olivier Bournez	Professeur à l'École Polytechnique	*rapporteur*
Bob Coecke	Professeur à l'Université d'Oxford	*examinateur*
Emmanuel Jeandel	Professeur à l'Université de Lorraine	*examinateur*
Elham Kashefi	Directrice de Recherche CNRS	*examinatrice*
Iordanis Kerenidis	Directeur de Recherche CNRS	*rapporteur*
Michele Pagani	Professeur à l'Université Paris Diderot	*rapporteur*

Laboratoire Lorrain de Recherche en Informatique et ses Applications – UMR 7503

Loria
Laboratoire lorrain de recherche en informatique et ses applications

Table des matières

Liste des tableaux

Résumé

L'informatique quantique est un sujet de recherche en plein essor. Un traitement quantique de l'information permet de résoudre des problèmes hors de portée des ordinateurs classiques. Il est essentiel de comprendre les structures fondamentales du traitement quantique de l'information pour développer des outils spécifiques et efficaces.

Dans cette thèse d'habilitation nous considérons plusieurs exemples d'approche graphique pour l'informatique quantique : tout d'abord le formalisme des états graphes, le calcul par mesure et le partage de secret de quantique.

Nous explorons ensuite en profondeur le ZX-calcul, un langage diagrammatique issue de la théorie des catégories qui permet de représenter et raisonner sur les évolutions quantiques. Ce langage est muni d'une théorie équationnelle permettant de transformer un diagramme en un diagramme équivalent. Le langage est dit complet si, pour toute paire de diagrammes représentant la même évolution quantique, il existe une transformation de l'un à l'autre en utilisant les règles du langage. Nous montrons la complétude du ZX-calcul pour plusieurs fragments de la mécanique quantique.

Abstract

Quantum computing is a fast-growing research area. A quantum computer can solve problems which are out of reach of the classical computers. It is essential to understand the fundamental structures of quantum information processing in order to develop specific and effective tools.

In this habilitation thesis we consider several examples of graphical approaches for quantum computing : first of all the graph state formalism, the measurement-based model of quantum computing and the quantum secret sharing protocol.

We then explore in depth the ZX-calculus, a category theory based diagrammatic language for quantum reasoning. This language is equipped with an equational theory to transform any diagram into an equivalent diagram. The language is said to be complete if, for any pair of diagrams representing the same quantum evolution, there exists a transformation from one to the other using the rules of the language. We show the completeness of ZX-calculation for several fragments of quantum mechanics.

Chapitre I

Bilan des activités de recherche

Dans ce chapitre, je présente rapidement mon parcours de chercheur depuis la fin de ma thèse. Je donne également une présentation synthétique de mon activité de recherche. Ces activités ont porté sur une approche graphique en informatique quantique avec principalement deux axes des recherche : (i) le formalisme des états graphes et leurs applications, notamment le calcul quantique par mesure et le partage de secret quantique ; (2) le ZX-calcul un langage graphique pour raisonner en informatique quantique.

Dans la suite de ce chapitre, mes contributions sur le premier axe sont présentées de façon synthétique, les contributions concernant le second axe seront présentées de façon plus approfondie dans les chapitres suivants. Nous supposons le lecteur familier avec les notions basiques d'informatique quantique comme les états quantiques (vecteurs normés d'un espace de Hilbert), les évolutions quantiques (unitaires, isométries, mesures), le formalisme des circuits quantiques et les notations de Dirac (*bra* et *ket*). En cas de besoin, une brève introduction à l'informatique quantique est donnée en annexe A.

I.1 Parcours de chercheur

Après ma thèse soutenue en 2006 à l'INP Grenoble, j'ai effectué un post-doc à Oxford dans le groupe de Samson Abramsky et Bob Coecke où j'ai découvert le ZX-calcul, un langage graphique pour l'informatique quantique qui était alors en cours de développement par Bob Coecke et Ross Duncan au Computing Laboratory d'Oxford. Après une année à Oxford j'ai effectué un postdoc joint entre le laboratoire PPS (Paris Diderot) et le LFCS de l'Université d'Edimbourg. Ce postdoc a été l'occasion de renforcer mes collaborations avec Elham Kashefi sur le calcul par mesures.

J'ai été recruté en 2009 au CNRS, affecté au LIG à Grenoble dans l'équipe CAPP. Avec Mehdi Mhalla et Pablo Arrighi nous avons encadré mon premier étudiant en thèse, Jérôme Javelle sur le partage de secret quantique. Quelques années plus tard, j'ai encadré avec Pablo Arrighi la thèse de David Cattanéo sur les problèmes de complexité associés aux états graphes.

En 2013, j'ai souhaité effectuer une mobilité au LORIA pour y développer une activité quantique au sein de l'équipe CARTE, avec Emmanuel Jeandel qui venait d'y être recruté comme Professeur des Universités. Mon activité s'est alors plus orientée vers le ZX-calcul, et notamment des questions fondamentales sur l'expressivité et la complétude de ce langage. Ces questions théoriques représentaient un verrou pour une utilisation plus large de ce langage graphique. Nous encadrons avec Emmanuel Jeandel depuis 2016 la thèse de Renaud Vilmart qui porte sur la complétude du ZX-calcul. Depuis septembre 2018, je co-encadre deux thèses supplémentaires, celle de Titouan Carette (avec Emmanuel Jeandel) et celle Robert Booth (avec Damain Markham, CR CNRS au LIP6).

Pour faire suite à l'équipe projet Inria CARTE, nous avons proposé une équipe projet Inria MOCQUA sur les modèles de calcul, notamment les modèles de calcul quantique, une thématique qui a été renforcée dans l'équipe avec l'arrivée de Frédéric Dupuis CR CNRS en 2017. Au niveau contractuel, je suis responsable du projet ANR SoftQPro (projet PRCE avec ATOS, Paris Sud et le CEA), je bénéficie également d'un financement Future Leader, une initiative de Lorraine Université d'Excellence. Je suis également responsable de workpackages dans d'autres projets : ANR VanQueTe, PRCI avec Singapour ; PIA-GDN/ Quantex ; et ECOS QuCa avec l'Argentine.

J'ai pris depuis quelques années des responsabilités nationales : je suis le responsable du groupe de travail Informatique Quantique (GT IQ) du GdR Informatique Mathématique depuis 2013 et membre du bureau du GdR IQFA depuis 2014. Le GT IQ et le GdR IQFA sont deux réseaux nationaux qui animent la communauté informatique quantique. En 2016, j'ai été élu secrétaire scientifique de la section 6 du CoNRS pour un mandat de 5 ans.

I.2 Recherche Scientifique

Une approche graphique pour l'informatique quantique. L'informatique quantique est un sujet de recherche en plein essor. Un traitement quantique de l'information permet en théorie de résoudre certains problèmes informatiques hors de portée des ordinateurs classiques. Il est essentiel de comprendre les structures fondamentales du traitement quantique de l'information pour développer des outils spé-

cifiques et efficaces. On constate que dans de nombreux domaines de l'informatique quantique une approche graphique s'est imposée. Le modèle des circuits quantiques [94] est par exemple un langage de bas niveau qui est pourtant largement plébiscité pour décrire des algorithmes quantiques. Les états graphes [53] qui consistent à représenter un état quantique par un graphe ont permis de mieux comprendre les propriétés de l'intrication, une corrélation forte qui n'a pas d'équivalent classique et qui est nécessaire à l'accélération des algorithmes quantiques. Calcul par mesures [82] et partage de secret [72, 48] sont d'autres exemples où une approche graphique permet de développer des outils efficaces pour étudier un modèle de calcul ou un protocole, et en comprendre les atouts et les limites. Enfin l'approche catégorique [2] de la mécanique quantique, notamment à travers le langage graphique ZX-calcul [28], a permis de mettre en évidence des structures fondamentales du traitement de l'information quantique qui peuvent être capturées graphiquement.

Circuits quantiques, états graphes et ZX-calcul sont donc des exemples de développements réussis de langages graphiques dans le traitement quantique de l'information. Il y a des raisons intrinsèques à ce succès : le picturalisme capture des propriétés quantiques fondamentales comme l'intrication, la contextualité, la causalité et la façon dont elles interagissent dans l'espace-temps.

Deux principaux axes de recherche. Mon activité de recherche s'est principalement portée sur deux axes :

Axe 1. Les états graphes et leurs applications, notamment le calcul quantique par mesure et le partage de secret quantique.

Axe 2. Les structures fondamentales du traitement de l'information quantique : ZX-calcul et axiomatisation catégorique.

Domaines scientifiques. Mon approche graphique de l'informatique quantique se décline en deux axes complémentaires qui sont ancrés dans des domaines assez différents de l'informatique "classique" : le premier axe comporte des connexions avec la théorie des graphes et de façon plus secondaire avec la complexité (quantique / classique), de la cryptographie et des modèles de calcul ; le second axe présente des liens avec les domaines de la théorie des catégories et de la sémantique.

La possibilité d'explorer (plus ou moins en profondeur) un large spectre des sciences de l'information est l'une des spécificités de l'informatique quantique que j'apprécie particulièrement. En effet, ce changement de paradigme (passage du classique au quantique) affecte potentiellement tous les domaines de l'informatique. Une autre spécificité de ce domaine est l'importance des interactions avec les physiciens. On peut distinguer deux types d'interactions : 1- sur les questions de physique fondamentale (axiomatisation de la mécanique quantique, étude de la causalité, la contextualité, l'intrication) ; 2- sur l'ingénierie quantique (essentiellement la construction

de l'ordinateur quantique). De façon peut-être surprenante l'interaction avec la physique fondamentale est souvent plus aisée, mais le contexte actuel du flagship européen et la maturité des technologies quantiques vont intensifier les interactions au niveau de l'ingénierie quantique dans un futur proche.

Mes contributions sur le premier axe sont présentées ci-dessous de façon synthétique alors les contributions concernant le second axe seront présentées plus en détails dans les chapitres suivants.

I.2.1 États graphes

Le formalisme des états graphes [53] permet de représenter un état quantique en utilisant un graphe où chaque sommet représente un bit quantique (qubit) et chaque arête représente intuitivement l'intrication entre ces qubits. Plus précisément, l'état d'un registre de n qubits est un vecteur normé dans un espace de Hilbert $\mathcal{H}$ de dimension 2^n. Étant donné un ensemble V de taille n, soit $\{\mathbf{e}_x, x \subseteq V\}$ (ou $\{|x\rangle, x \subseteq V\}$ en notation de Dirac) une base orthonormée de $\mathcal{H}$.

Tout état $|\phi\rangle$ d'un registre de n qubits peut donc s'écrire $\sum_{x\subseteq V} \alpha_x |x\rangle$ avec $\sum_{x\subseteq V} |\alpha_x|^2 = 1$. Un graphe $G = (V, E)$ représente l'état quantique

$$|G\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\subseteq V} (-1)^{|G[x]|} |x\rangle$$

où $|G[x]|$ est le nombre d'arêtes du sous graphe de G induit par x.

Le formalisme des états graphes permet une représentation compacte des états quantiques. En effet, la description d'un état quantique quelconque nécessite 2^n nombres complexes alors qu'un état graphe sur n qubits est entièrement caractérisé par $n(n-1)/2$ bits. La contre partie est que seuls quelques états quantiques peuvent être représentés par des graphes. Il s'avère que cette sous famille d'états quantiques est particulièrement représentative et intéressante. Elle est utilisée dans de nombreuses applications en traitement de l'information quantique, notamment pour l'étude de modèles de calcul quantique [80], en cryptographie quantique [73] ou encore pour les codes correcteurs d'erreurs quantiques [84]. Le succès de ce formalisme est non seulement dû au fait que les états graphes sont très prometteurs en terme d'implémentation physique [92, 79], mais aussi dû à l'opportunité de caractériser de façon combinatoire certaines propriétés quantiques.

Mes activités de recherche dans cet axe ont principalement pour objectif de caractériser de façon combinatoire les différentes propriétés des états graphes pour mieux comprendre les capacités et les limites des états graphes dans leurs nombreuses applications en traitement de l'information quantique.

I.2.2 États graphes et calcul par mesure

Historiquement, l'une des premières applications des états graphes a été le calcul par mesure [81]. Il s'agit essentiellement d'effectuer un calcul en mesurant successivement les qubits d'un état graphe. Le résultat du calcul dépend du graphe, des bases des différentes mesures et aussi de l'ordre dans lequel sont effectuées les mesures. Le calcul par mesure est un modèle de calcul alternatif au modèle 'standard' des circuits quantiques.

Profondeur quantique. Le calcul par mesure est très prometteur en terme d'implémentation physique [79, 92]. Ce modèle est également intéressant d'un point de vu théorique, l'utilisation de ce modèle permettant de diminuer la profondeur quantique de certains algorithmes par rapport au modèle standard des circuits quantiques. En effet, dès l'introduction de ce modèle, Raussendorf et Briegel [80] ont noté que certaines opérations quantiques, dites de *Clifford*, peuvent être exécutées en profondeur constante (i.e. en temps constant dans le cadre d'une exécution parallèle). Broadbent et Kashefi [21] ont mis en évidence une séparation avec le modèle des circuits quantiques en démontrant que le problème de PARITÉ (n bits $x_1, \dots x_n$ en entrée, $\sum x_i \bmod 2$ en sortie) nécessite des circuits quantiques de profondeur $\Omega(\log(n))$ alors qu'il existe une exécution en profondeur quantique $O(1)$ dans le modèle du calcul par mesure.

Avec Dan Browne et Elham Kashefi [23] nous avons montré que le modèle du calcul par mesure est en fait équivalent à celui des circuits quantiques avec fan-out non borné [55], montrant par conséquence que la transformée de Fourier quantique peut être implémentée en profondeur quantique constante et que l'algorithme de factorisation de Shor peut être exécuté en temps polynomial sur un ordinateur classique probabiliste associé à un ordinateur quantique effectuant uniquement des calculs de profondeur quantique constante.

Nous avons mis en évidence que la supériorité du calcul par mesure face aux circuits quantiques vient de la nature hybride classique/quantique du modèle et de l'hypothèse que la profondeur de la partie classique est négligée (alors qu'elle peut être jusqu'à logarithmique). En substance, nous avons montré que le modèle de calcul par mesure permet de transformer une partie des opérations quantiques en opérations classiques diminuant d'autant la profondeur de la partie quantique restante.

Ce résultat est particulièrement important pour l'implémentation de l'ordinateur quantique, qui sera selon la plupart des propositions d'architecture actuelles, une machine hybride associant un ordinateur classique contrôlant une unité quantique. Ce résultat ouvre également de nouvelles perspectives vers une éventuelle preuve de la conjecture de Jozsa [65] : *"Any polynomial time quantum algorithm can be*

implemented with only O(log n) quantum layers interspersed with polynomial time classical computations. "

Déterminisme et préservation de l'information. Les états graphes sont les ressources du calcul par mesure. Une propriété remarquable du calcul par mesure est que bien que l'opération de base dans ce modèle soit la mesure quantique qui possède une évolution fondamentalement probabiliste, des évolutions globalement déterministes peuvent être obtenues, notamment dans le cas de la simulation de circuits quantiques. La capacité à obtenir une évolution déterministe est due à l'utilisation de mesures adaptatives : la base d'une mesure effectuée à l'étape i dépend des résultats (probabilistes) des mesures précédentes. L'existence de telles mesures adaptatives dépend de la structure du graphe. Danos et Kashefi [34] ont montré que l'existence d'un flot de causalité dans le graphe est une condition suffisante à un tel déterminisme. En 2007, nous avons montré avec Browne, Kashefi et Mhalla [22] que le déterminisme dans ce modèle est caractérisé par la notion de *gflow*. Avec Mhalla en 2008 [75] nous avons introduit un algorithme polynomial qui permet de décider si un graphe admet un *gflow*.

Universalité des grilles triangulaires et pivot mineur. Dans le papier séminal de Briegel et Raussendorf [80], les auteurs ont montré que tout cricuit quantique peut être simulé en utilisant uniquement des états graphes associés à des grilles. Ainsi la famille des grilles forme une ressource universelle pour le calcul par mesure. Plusieurs autres familles de graphes ont été montrées universelles [91, 20]. Avec Mehdi Mhalla [76] nous avons montré que les grilles triangulaires sont universelles avec comme contrainte supplémentaire que toutes les mesures effectuées pendant le calcul sont décrites par des observables réels. Nous avons également montré que tout graphe est pivot mineur d'une grille triangulaire. Ces deux résultats, l'un 'quantique' l'autre 'classique' sont les deux faces d'une même pièce, dont la preuve est une combinaison d'arguments de théorie des graphes et d'information quantique.

I.2.3 Partager un secret à l'aide d'un état graphe

Contexte. Un protocole de partage d'un secret s parmi n joueurs possède un seuil k si tout ensemble d'au moins k joueurs peut reconstruire le secret s alors que tout ensemble de moins de k joueurs n'a aucune information sur le secret s. Shamir [89] a montré que pour tout nombre de joueurs n et pour tout seuil $k \leq n$, il existe un protocole permettant de partager le secret (classique) s. Quand le secret est un état quantique le seuil ne peut être inférieur à $n/2$. En effet, dans le cas contraire, deux ensembles distincts de joueurs pourraient reconstruire le secret, menant à une duplication du secret, violant ainsi le théorème de non-clonage [93]. En revanche,

pour tout seuil $k > n/2$, Gottesman [46] a montré l'existence d'un protocole de partage de secret permettant de partager un secret quantique parmi n joueurs avec un seuil k. Ces protocoles de partage de secret quantique souffrent malheureusement d'un inconvénient : la taille du système quantique donné à chaque joueur croît linéairement avec le nombre total de joueurs.

Markham et Sanders [73] ont proposé une nouvelle famille de protocoles de partage de secret quantique utilisant des états graphes. Chacun de ces protocoles est caractérisé par un graphe. Étant donné un graphe G d'ordre n, le secret quantique $\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ est encodé dans l'état $\alpha\,|G\rangle + \beta\,|G'\rangle$ où G' est le graphe obtenu à partir de G en ajoutant des boucles à chaque sommet de G qui n'en possédait pas et en supprimant celles qui existaient. Chaque qubit de cet état est alors envoyé à un joueur. Ce protocole possède le double avantage (i) d'utiliser des états graphes très prometteurs en terme d'implémentation physique et (ii) de garantir que chaque joueur possède un unique qubit, contrairement au protocole proposé par Gottesman. Markham et Sanders ont montré que le pentagone (C_5) permet de réaliser un protocole à 5 joueurs ayant un seuil 3 et que les graphes complets réalisent des protocoles d'unanimité (i.e. le seuil est égal au nombre de joueurs). À noter qu'un protocole équivalent à ce dernier protocole d'unanimité a indépendamment été proposé par Broadbent, Chouha et Tapp [19].

Notre objectif a été de déterminer les possibilités et les limites de ces protocoles prometteurs : quels seuils peuvent être réalisés en utilisant un protocole à base d'état graphe ?

Caractérisation graphique. Afin d'étudier cette famille de protocoles nous avons dans un premier temps introduit une caractérisation graphique des ensembles de joueurs ayant accès au secret quantique [67, 56]. Cette caractérisation graphique peut être décrite en terme de domination impaire [1] dans le graphe : étant donné un graphe $G = (V, E)$, un ensemble $B \subseteq V$ de joueurs peut accéder au secret quantique si et seulement si B n'est pas dominé de façon impaire et que $V \setminus B$ l'est.

Protocoles de quasi-unanimité. L'existence d'une telle caractérisation graphique est cruciale pour l'étude de ces protocoles : elle nous a permis de montrer que pour tout n et pour tout $k \geq n - n^{0.71}$, il existe un graphe qui réalise un protocole de partage de secret quantique à n joueurs dont le seuil est k [56]. De tels protocoles sont dits de *quasi-unanimité* car k/n tend vers 1 quand $n \to \infty$. Ce résultat est constructif : un tel graphe est essentiellement obtenu par le produit lexicographique

1. Un ensemble A de sommets est dominé de façon impaire s'il existe $C \subseteq V \setminus A$ tel que pour $\forall u \in A$, u a un nombre impair de voisins dans C.

successif d'un graphe de Paley. Nous avons mis en évidence que les graphes de Paley constituenet une famille particulièrement intéressante pour le partage de secret quantique. Les sommets d'un graphe de Paley sont les éléments d'un corps fini, deux sommets sont reliés par une arête si et seulement si leur différence est un résidu quadratique.

Protocoles à seuil 'linéaire'. Aucune construction connue ne permet d'obtenir des protocoles à base d'état graphe ayant un seuil 'linéaire', i.e. tel que $k/n \to c$ quand $n \to \infty$ où n est le nombre de joueurs, k le seuil et $c < 1$ une constante. En revanche, en utilisant des méthodes probabilistes, plus particulièrement le lemme local de Lovász, nous avons démontré que pour tout n et tout $k \geq 0.811n$ il existe un graphe réalisant un protocole de partage de secret quantique à n joueurs dont le seuil est k [56]. En fait nous avons montré que la plupart des graphes permet de réaliser un seuil linéaire : si G est un graphe aléatoire (chaque paire de sommets est reliée par une arête avec probabilité 0.5), alors le seuil du protocole correspondant est inférieur à $0.811n$ avec probabilité $1 - 1/n$. Par conséquent, même si la méthode n'est pas constructive, un graphe choisi aléatoirement produira un bon protocole avec grande probabilité.

Borne inférieure. Nous avons également démontré un résultat d'impossibilité : il n'existe pas de protocole à base d'état graphe permettant d'atteindre un seuil inférieur à $0.506n$ [56]. L'existence de protocole à base d'états graphe pour des seuils compris entre $0.506n$ et $0.811n$ reste ouverte (voir Figure I.1).

Extension au partage de secret avec des multi-graphes. Avec Anne Marin et Damian Markham [71] nous avons montré que les bornes inférieures et supérieures s'étendent au cas du partage de secret à l'aide de *qudit-graph states*. Un qudit-graph state est une généralisation des états graphes où chaque sommet représente un système quantique de dimension d fixée, où d est une puissance de nombre premier. L'état quantique est alors représenté par un multigraphe où chaque paire de sommets est connectée par au plus $d - 1$ arêtes. Le partage de secret quantique à base de qudit-graph states a été introduit par Keet et al. [68]. Nous avons proposé une caractérisation graphique des ensembles accessibles pour ces protocoles et donné des bornes sur les seuils de tels protocoles. Ces bornes généralisent le cas binaire, et tendent vers un seuil de 50% des joueurs quand la dimension d des qudits tend vers l'infini.

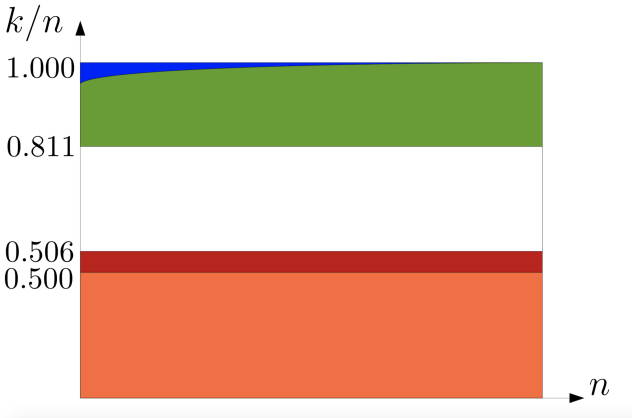


FIGURE I.1 – Existence de partage de secret quantique à base de graphe, réalisant un certain ratio k/n en fonction de n où n est le nombre de joueurs et k est le seuil. La zone bleue représente les protocoles constructifs connus. Ces protocoles sont des protocoles de quasi-unanimité ($k/n \to 1$). La zone verte correspond à l'existence non constructive de protocole de partage de secret quantique. La zone orange correspond à la zone interdite par le théorème de non clonage, enfin la zone rouge est la zone interdite par notre nouvelle borne inférieure. L'existence de protocole dans la zone blanche est un problème ouvert.

I.2.4 Complexité des problèmes associés aux états graphes

Partage de secret quantique à base de graphes, et problèmes de domination. Dans le cadre du partage de secret quantique à base de graphes, nous avons montré qu'un graphe aléatoire produit un protocole à seuil linéaire avec grande probabilité. En répétant le processus en cas d'échec, on obtient en un nombre espéré constant de générations de graphes aléatoires un protocole ayant un seuil linéaire. Il est donc crucial d'étudier la complexité du problème consistant à décider si le seuil associé à un graphe est inférieur ou égal à une valeur donnée. Nous avons montré que ce problème de décision est malheureusement NP-complet [48, 47]. En effet le problème de décision associé au calcul du seuil d'un protocole peut être reformulé en une variation du problème de domination dans un graphe : la domination impaire faible. Étant donné un graphe G, un sous ensemble B de sommets est WOD (pour *weak odd dominated*) s'il existe un ensemble D de sommets distinct de B tel que tout sommet dans B est relié à un nombre pair de sommets dans D. Nous avons montré la NP-complétude de la domination impaire faible en réduisant ce problème de l'existence d'un code parfait dans un graphe régulier, prouvé NP-complet par Kratochvil [70].

Avec David Cattanéo, dont j'ai co-encadré la thèse, nous avons étudié la complexité paramétrée de ce problème. Ce problème est dans W[2] et W[1]-difficile, ce qui signifie, sous l'hypothèse $W[1] \neq FPT$ que ce problème ne peut pas être résolu efficacement même à paramètre fixé (i.e. il n'est pas *fixed parameter tractable*) [24]. Plus précisément nous avons montré que le problème associé au calcul du seuil d'un protocole est FPT-équivalent au problème OddSet, introduit par Downey et al. [38] connu comme étant W[1]-difficile et dans W[2].

Nous avons à cette occasion développé une nouvelle caractérisation de la classe W[2] à base de Machine de Turing. Plus précisément nous avons généralisé la caractérisation de Cesati [26] à base de Machine de Turing multi-ruban en ajoutant à ces machines la possibilité de faire des transitions 'à l'aveugle', c'est à dire en ignorant tout ou partie des symboles lus par les têtes de la machine. Cette nouvelle machine nous a permis de démontrer l'appartenance à W[2] de plusieurs problèmes liés à la domination impaire dans les graphes, mais plus généralement de la $[\sigma, \rho]$-domination introduite par Telle [90]. Étant donnés deux sous-ensembles σ et ρ d'entiers, un graphe G et un sous ensemble D de sommets, D est $[\sigma, \rho]$-dominant si pour tout sommet u du graphe, si $u \in D$ alors $|N(u) \cap D| \in \sigma$, sinon $|N(u) \cap D| \in \rho$. Le choix des paramètres σ et ρ permet de décrire une grande classe de problèmes sur les graphes : domination, ensemble indépendant, code parfait, et aussi d'étudier comment la complexité, notamment la complexité paramétrée, dépend des paramètres σ et ρ. Citons par exemple le résultat de Golovach, Kratochvíl, and Suchý [45] montrant que si σ et ρ sont deux ensembles finis non vides alors le problème de décision

associé à la $[\sigma, \rho]$-domination est W[1]-difficle. En appliquant la caractérisation de W[2] à base de machines de Turing que nous avons introduite, nous avons montré que pour tout σ et ρ calculables le problème de $[\sigma, \rho]$-domination est dans $W[2]$.

Degré minimal à complémentation locale près. En 2006, avec Peter Høyer et Mehdi Mhalla [54] nous avons montré que la complexité de préparation d'un état graphe (i.e. le nombre d'opérations permettant de produire l'état graphe $|G\rangle$ à partir de la description du graphe G) dépend du degré minimum à complémentation locale près, noté δ_{loc}. La complémentation locale, introduite par Bouchet [18], possède des propriétés remarquables pour les états graphes : deux graphes localement équivalents (i.e. on peut transformer l'un en l'autre par une suite de complémentations locales) possèdent la même intrication. Le plus petit degré à complémentation locale près s'est depuis révélé être un paramètre important pour les états graphes dans d'autres applications. δ_{loc} et le seuil des protocoles de partage de secret quantique sont par exemple liés : le seuil d'un protocole associé à un graphe G d'ordre n est supérieur $n - \delta_{loc}(G)$.

La construction de famille de graphes ayant un grand δ_{loc} est donc un point important en traitement de l'information quantique. L'hypercube d'ordre n a un δ_{loc} logarithmique [54]. Nous avons montré avec Jérome Javelle et Mehdi Mhalla [57] que pour tout graphe de Paley P_n d'ordre n, $\delta_{loc}(P_n) \geq \sqrt{n}$. De plus nous avons montré, en utilisant des méthodes probabilistes, l'existence de graphes dont le δ_{loc} est supérieur à $0.188n$ où n est l'ordre du graphe. Nous avons également montré qu'il existe des graphes bipartis dont le δ_{loc} est supérieur à $0.12n$. Enfin, en terme de complexité, le problème de décision associé au δ_{loc} est NP-complet, même sur les graphes bipartis ; de plus nous avons montré que cette quantité est difficile à approximer. Avec David Cattanéo [25] nous nous sommes ensuite intéressés à la complexité paramétrée de ce problème et nous avons montré que, même dans le cas des graphes bipartis, ce problème est FPT-équivalent au problème EvenSet [38]. Ce problème est dans la classe W[2], en revanche savoir si ce problème est W[1]-difficile est une question ouverte.

Nous avons également amélioré les bornes supérieures connues sur le degré minimum à complémentation locale près [25]. Il est assez simple de montrer que δ_{loc} est au plus la moitié des sommets du graphe. Nous avons montré que cette quantité est en fait inférieure à $3n/8 + o(n)$ et même inférieure à $n/4 + o(n)$ quand le graphe est bipartite, où n est le nombre de sommets du graphe. Nous en avons déduit que le degré minimum à complémentation locale près peut être calculé par un algorithme exact mais exponentiel, en temps $O^*(1.938^n)$, ($O^*(1.466^n)$ dans le cas biparti).

Chapitre II

Introduction au ZX-calcul

Nous donnons dans ce chapitre une introduction au ZX-calcul, un puissant calcul graphique permettant de raisonner en informatique quantique. Ce langage est central dans ce mémoire. Comme dans le chapitre précédent, nous supposons le lecteur familier avec les notions de base d'informatique quantique qui sont rappelées en annexe A.

II.1 ZX-calcul, un langage graphique pour l'informatique quantique

Le ZX-calcul, introduit par Coecke et Duncan [28] est un langage graphique puissant pour raisonner en informatique quantique. Le ZX-calcul est issu du programme "mécanique quantique catégorielle"[1] inititié par Abramsky and Coecke [3], qui a donné lieu a un domaine de recherche fertile. Le ZX-calcul est le langage graphique qui permet de représenter et de manipuler les états quantiques et les évolutions quantiques. Il s'agit de diagrammes de cordes (string diagrams) qui peuvent être décrits dans un contexte catégorique. Nous faisons le choix dans ce document de présenter le ZX-calcul comme un langage graphique, sans utiliser le formalisme catégorique. C'est un choix qui a pour but de rendre accessible le formalisme du ZX-calcul aux non spécialistes de théorie des catégories, afin de faciliter la démocratisation de ce langage dans la communauté du traitement de l'information quantique. La contrepartie de ce choix est sans doute une perte d'élégance, de profondeur et d'abstraction pour certains résultats qui pourraient être présentés dans un formalisme catégoriel.

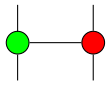
Le ZX-calcul peut être vu comme une généralisation des circuits quantiques, en plus expressif. On peut représenter des transformations unitaires sur 1 qubit comme

1. "categorical quantum mechanics"

la transformation d'Hadamard (H), les rotations autour de l'axe X et Z ($R_X(\alpha)$, $R_Z(\alpha)$), et T la rotation autour de Z d'angle $\frac{\pi}{4}$.

$H :$ $\quad R_Z(\alpha) :$ $\quad R_X(\alpha) :$ $\quad T :$ 

ou encore des opérations sur deux qubits comme CNot (*Control-Not*) :

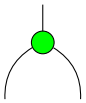
$\Lambda X :$ 

À noter que les diagrammes du ZX-calcul se lisent du haut vers le bas.

Des évolutions non unitaires peuvent également être représentées comme des états quantiques :

$|0\rangle :$  $\quad |1\rangle :$  $\quad |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} :$  $\quad \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) :$ 

ou des isométries comme la copie dans la base standard :

$$\begin{array}{ccc} |0\rangle & \mapsto & |00\rangle \\ |1\rangle & \mapsto & |11\rangle \end{array} :$$ 

Le ZX-calcul permet également la représentation d'évolutions qui ne sont pas des isométries, comme une mesure de Bell post-sélectionnée, c'est-à-dire une projection sur l'état $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$$\frac{1}{\sqrt{2}}(\langle 00| + \langle 11|) :$$ 

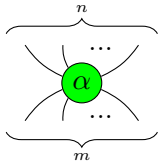
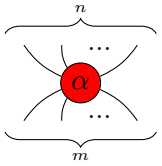
ou une mesure post sélectionnée dans la base computationnelle

$\langle 0| :$  $\quad \langle 1| :$ 

Dans la suite, nous décrivons la syntaxe et la sémantique des diagrammes du ZX-calcul.

II.1.1 ZX-diagrammes : syntaxe et sémantique

Un ZX-diagramme $D : k \to l$ avec k entrées et l sorties est généré par :

$R_Z^{(n,m)}(\alpha) : n \to m$		$R_X^{(n,m)}(\alpha) : n \to m$	
$H : 1 \to 1$		$e : 0 \to 0$	
$\mathbb{I} : 1 \to 1$		$\sigma : 2 \to 2$	
$\epsilon : 2 \to 0$		$\eta : 0 \to 2$	

où $m, n \in \mathbb{N}$ et $\alpha \in [0, 2\pi)$

— Composition spatiale : pour tout $D_1 : a \to b$ et $D_2 : c \to d$, $D_1 \otimes D_2 : a+c \to b+d$ consiste à placer D_1 et D_2 côte à côte, D_2 à la droite du D_1.

— Composition séquentielle : pour tout $D_1 : a \to b$ et $D_2 : b \to c$, $D_2 \circ D_1 : a \to c$ consiste à placer D_1 au dessus de D_2, en reliant les sorties D_1 aux entrées D_2.

Les angles des points verts ou rouges sont omis quand ils sont égaux à 0 modulo 2π :

L'interprétation standard des ZX-diagrammes associe à tout diagramme $D : n \to m$ une application linéaire $[\![D]\!] : \mathbb{C}^{2^n} \to \mathbb{C}^{2^m}$ définie inductivement comme suit :

$$[\![D_1 \otimes D_2]\!] := [\![D_1]\!] \otimes [\![D_2]\!] \qquad [\![D_2 \circ D_1]\!] := [\![D_2]\!] \times [\![D_1]\!]$$

$$[\![$$  $]\!] := 1 \qquad [\![$  $]\!] := |0\rangle\langle 0| + |1\rangle\langle 1|$$

$$[\![$$  $]\!] := |+\rangle\langle 0| + |-\rangle\langle 1| \qquad [\![$  $]\!] := \sum_{i,j \in \{0,1\}} |ij\rangle\langle ji|$$

$$[\![$$  $]\!] := |00\rangle + |11\rangle \qquad [\![$  $]\!] := \langle 00| + \langle 11| \qquad [\![$  $]\!] = [\![$  $]\!] := 1 + e^{i\alpha}$$

Pour tout n, m tels que $n + m > 0$:

$$[\![$$  $]\!] := |0^m\rangle\langle 0^n| + e^{i\alpha}\,|1^m\rangle\langle 1^n| \qquad [\![$  $]\!] := |+^m\rangle\langle +^n| + e^{i\alpha}\,|-^m\rangle\langle -^n|$$

Les diagrammes du ZX-calcul sont universels dans le sens où toute transformation linéaire peut être représentée par un ZX-diagramme :

Propriété II.1.1 (Universalité [28]). *Pour tout $n, m \in \mathbb{N}$, et toute transformation linéaire $A \in \mathbb{C}^{2^n} \to \mathbb{C}^{2^m}$, il existe un ZX-diagramme $D : n \to m$ tel que $[\![D]\!] = A$.*

En particulier toute transformation unitaire sur un nombre fini de qubit peut être représentée par un ZX-diagramme.

Le fragment stabilisable de la mécanique quantique est formé des évolutions quantiques obtenues à partir d'initialisation de qubit dans l'état $|0\rangle$, d'opérations de Clifford (générées par H, Z, ΛX) et de mesure post-sélectionnées dans la base standard. Ce fragment correspond au fragment $\frac{\pi}{2}$ du ZX-calcul, i.e. tous les diagrammes dont les angles sont des multiples de $\frac{\pi}{2}$.

Le fragment Clifford+T de la mécanique quantique correspond lui au fragment $\frac{\pi}{4}$ du ZX-calcul. Ce fragment est approximativement universel :

Propriété II.1.2 (Universality [28]). *Pour tout $n, m \in \mathbb{N}$, toute matrice $A \in \mathbb{C}^{2^n} \to \mathbb{C}^{2^m}$ et tout $\epsilon > 0$ il existe un diagramme $D : n \to m$ dans le fragment $\pi/4$ du ZX-calcul tel que $||[\![D]\!] - A|| \leq \epsilon$, avec $||U|| := \sup_{|\phi\rangle, \langle\phi|\phi\rangle \neq 0} \sqrt{\langle\phi| U^\dagger U |\phi\rangle}$.*

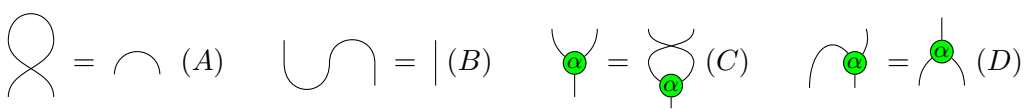
II.1.2 ZX-calcul : théorie équationnelle

La représentation d'une transformation linéaire dans ce langage graphique n'est pas unique : deux ZX-diagrammes différents peuvent représenter la même évolution quantique. Les ZX-diagrammes sont donc équipés d'une théorie équationnelle qui forme le ZX-calcul proprement dit. On écrira $ZX \vdash D_1 = D_2$ quand D_1 peut être réécrit en D_2 en utilisant les équations du langage.

Nous présentons ci-dessous certaines de ces équations. Toutes préservent la sémantique des diagrammes : si on peut transformer un diagramme D_1 en un diagramme D_2 en utilisant une de ces transformations (i.e. $ZX \vdash D_1 = D_2$) alors D_1 et D_2 représentent la même évolution (i.e $[\![D_1]\!] = [\![D_2]\!]$).

Seule la connexité compte

Les premières équations du langage peuvent être regroupées dans une méta-règle : "seule la connectivité compte" [28], en d'autres termes, un ZX-diagramme peut être déformé sans changer son interprétation. Elle implique notamment :



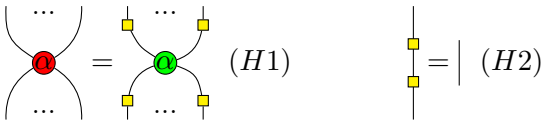
C'est une propriété fondamentale qui justifie l'approche graphique en informatique quantique. Les diagrammes peuvent être déformés à souhait transformant des

entrées en sorties. Par exemple l'équation (B) peut être vue comme la téléportation post-sélectionnée : à gauche il y 3 qubits dont deux sont initialisés dans l'état intriqué $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$, on applique ensuite une mesure de Bell sur deux d'entre eux. La téléportation post sélectionnée est ici trivialisée par l'utilisation du langage graphique.

La méta-règle : "seule la connectivité compte" implique que les ZX-diagrammes peuvent être vus comme des graphes au sens de la théorie des graphes, i.e. un ensemble de sommets (de trois couleurs différentes : rouges, verts ou jaunes), et des arêtes connectant ces sommets et des demi-arêtes pour les entrées et sorties.

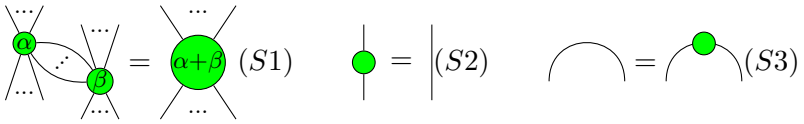
Échange de couleur

Une équation préserve la sémantique si et seulement si l'équation obtenue en échangeant les couleurs rouge et verte préserve la sémantique. C'est une conséquence directe des deux règles suivantes :



Fusion de nœuds

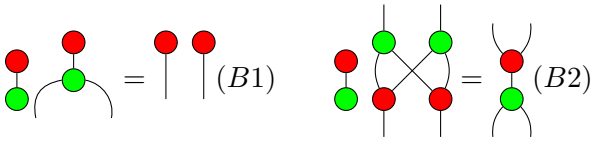
Une première transformation, qui ne correspond pas simplement à deformer un diagramme, consiste à fusionner des sommets. Cette règle appelée *spider* (S1) indique que toute paire de nœuds voisins de même couleur peut être fusionnée. De plus, un nœud de degré deux et un angle 0 peut être enlevé selon les règles (S2) ou (S3). Ces règles trouvent leur origine dans l'axiomatisation des bases orthonormées. Les nœuds verts correspondent à la base standard $\{|0\rangle, |1\rangle\}$, les nœuds rouges à la base $\{|+\rangle, |-\rangle\}$ et plus généralement pour toute base orthonormée on peut définir des nœuds satisfaisant ces équations de fusion. Coecke, Pavlovic et Vicary [32] ont montré qu'il s'agit ici d'une caractérisation : si une famille d'applications linéaires satisfait les équations de fusion alors elles correspondent à une base orthonormée.



Interactions entre les couleurs

Les diagrammes monochromatiques sont peu expressifs : selon la règle (S1), tout diagramme monochromatique (vert ou rouge) connecté équivaut à un seul point

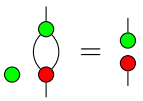
avec le nombre approprié de branches et dont l'angle est la somme des angles. Ainsi, les structures intéressantes apparaissent lorsque les deux couleurs interagissent. La règle (B1) est appelée *copie*, en effet, si on ignore le scalaire (digramme sans entrée-sortie qui représente juste une renormalisation), le nœud rouge est 'copié' par le nœud vert. La règle (B2), appelée *bigèbre*, est une règle de commutation : appliquer une co-copie (i.e. l'adjoint d'une copie) rouge, suivie d'une copie verte (à droite de l'équation) est équivalent, à un scalaire près, à d'abord appliquer la copie verte sur chacun des qubits, puis à appliquer des co-copies rouges.



Les règles de copie (B1) et bigèbre (B2), impliquent que les bases rouge et verte sont complémentaires, ou non-biaisées, ce qui intuitivement capture la notion de principe d'incertitude, une propriété fondamentale de l'information quantique (voir [28] pour plus de détails).

Arêtes parallèles et loi de Hopf

En combinant les règles (B1), (B2) et (S3) on peut démontrer l'équation suivante, appelée loi de Hopf :

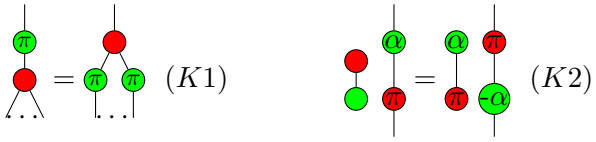


(II.1)

La loi de Hopf a alors une signification graphique simple : deux fils parallèles entre des points de couleurs distinctes peuvent être supprimés (au scalaire ● près).

π-commutation et π-copie

Toutes les règles du ZX-calcul présentées jusqu'ici étaient soit valables pour des angles arbitraires, soit spécifiques à l'angle nul (représenté par des nœuds sans angle). Nous présentons maintenant des règles spécifiques à l'angle π. En effet les nœuds d'angle π ayant une entrée et une sortie sont des opérateurs de Pauli, dont les propriétés sont remarquables. Par exemple un opérateur de Pauli est *copié* par un nœud de couleur opposé (K1) et vérifie une propriété de commutation avec un nœud de couleur opposé ayant un angle arbitraire (K2) :

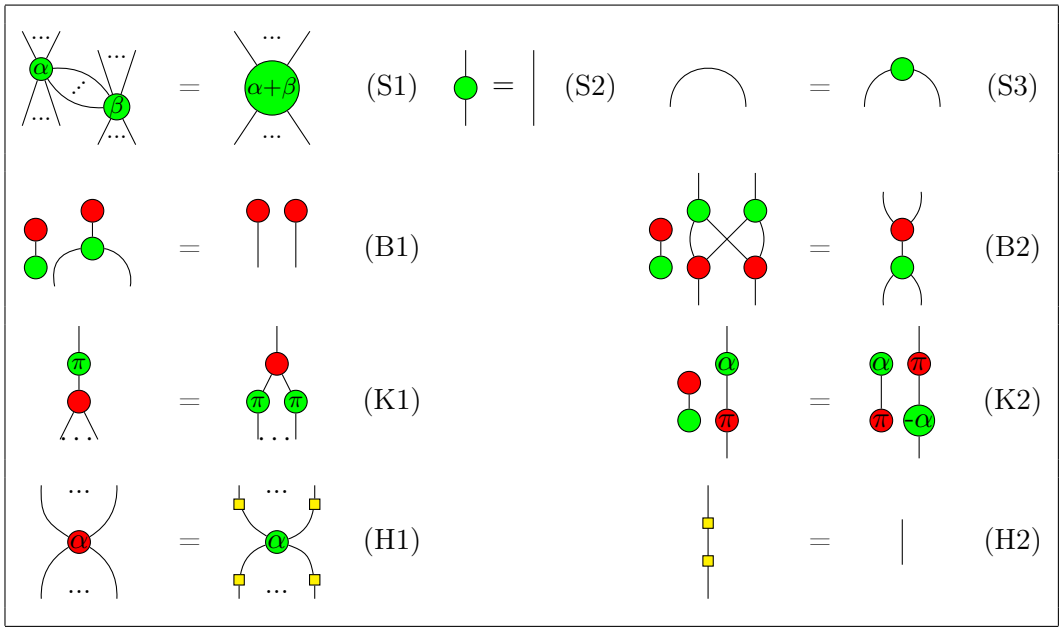


Contexte.

Les équations présentées ci-dessus peuvent être appliquées à n'importe quel sous-diagramme. En d'autres termes, si $ZX \vdash D_1 = D_2$ alors, pour tout D (avec le nombre approprié d'entrées/sorties), $ZX \vdash D \otimes D_1 = D \otimes D_2$; $ZX \vdash D_1 \otimes D = D_2 \otimes D$; $ZX \vdash D \circ D_1 = D \circ D_2$; et $ZX \vdash D_1 \circ D = D_2 \circ D$.

II.1.3 ZX$_0$-calcul

Nous résumons ici les règles originelles du ZX-calcul que nous appelons ZX_0.



À noter que ces règles diffèrent légèrement des règles originales [28] qui ne possédaient pas de scalaires, c'est-à-dire des diagrammes sans entrée ni sortie comme dans les règles (B1), (B2) ou (K2). Ces scalaires indispensables pour que les règles préservent la sémantique, étaient omis dans les premières versions du ZX-calcul car la correction des équations y était définie de façon plus faible. Dans cette version

plus faible les règles sont correctes si elles préservent la sémantique à un facteur multiplicatif non nul près.

II.2 Variantes du ZX-calcul

Depuis l'introduction du ZX-calcul, plusieurs variantes de ce langage ont été introduites.

II.2.1 Mécanique quantique pure à base de qubits

Le ZX-calcul est un langage pour la mécanique quantique pure (sans mesure) dont la brique de base est le qubit. Il existe plusieurs variantes du ZX-calcul pour ce fragment de la mécanique quantique :

ZW-calcul : un langage pour l'intrication

Coecke et Kissinger ont introduit le GHZ/W-calcul [30] qui a ensuite donné naissance au ZW-calcul [51]. La motivation de cette introduction est la représentation de l'intrication. En effet il existe seulement deux types d'états intriqués sur 3 qubits, ceux qui sont SLOCC [2]-équivalents à l'état $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, et ceux qui sont SLOCC-équivalents à $|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$. Alors que l'état $|GHZ\rangle$ se représente très simplement en ZX-calcul, il n'y a pas de représentation simple d'un état $|W\rangle$. L'idée du ZW-calcul est de proposer comme générateurs du langage ces deux états $|GHZ\rangle$ et $|W\rangle$. Le ZW-calcul a ensuite été développé par Amar Hadzihasanovic comme un langage graphique pour représenter des matrices à coefficients entiers [50]. Plus récemment le langage a été étendu pour représenter des matrices sur un anneau commutatif quelconque [51, 52], en particulier $\mathbb{C}$. Nous décrivons succinctement le ZW-calcul en section IV.1.4.

ZH-calcul : une extension aux états hypergraphes

Récemment, Backens et Kissinger ont introduit le ZH-calcul [9]. Il s'agit d'une variante du ZX-calcul où les boites Hadamard peuvent être d'arité quelconque. Alors que le ZX-calcul permet de représenter de façon très naturelle les états graphes, le ZH-calcul permet de représenter les états hyper-graphes [83], une généralisation des états graphes.

2. stochastic local operations and classical communications

Fragment réel et Y-calcul

Alors que le ZX-calcul est universel pour la mécanique quantique *complexe* (en fait on peut représenter toute matrice $2^n \times 2^m$ dont les coefficients sont des nombres complexes), il est intéressant, notamment d'un point de vue des fondements de la mécanique quantique, de considérer la mécanique quantique réelle, correspondant à des matrices à coefficients réels. À noter que les mécaniques quantiques réelle et complexe ont la même puissance computationnelle : si un problème peut être résolu par un circuit quantique (complexe) avec t portes et n qubits, alors il existe un circuit quantique pour résoudre ce problème avec $O(t)$ portes réelles et $n+1$ qubits.

Avec Ross Duncan, nous avons étudié un fragment réel du ZX-calcul [41], que nous avons étendu avec Emmanuel Jeandel et Renaud Vilmart en un langage universel pour la mécanique quantique réelle, appelé le Y-calcul [59]. Il s'agit du fragment sans angle du ZX-calcul augmenté d'une rotation réelle, la rotation autour de l'axe Y de la sphère de Bloch, d'où le nom du langage.

Un ZX-calcul avec plus de générateurs

Kang Feng NG et Harny Wang ont introduit une variante du ZX-calcul qu'ils ont montrée complète. Il s'agit d'une extension du ZX-calcul avec deux générateurs supplémentaires, que nous appellerons respectivement 'triangle' et 'λ-box'. Le triangle a été introduit pour la première fois dans la preuve de complétude du ZX-calcul pour le fragment $\frac{\pi}{4}$ (voir section IV.2.1). Le triangle était alors simplement un sucre syntaxique. La preuve de complétude de Kang Feng NG et Harny Wang s'appuie sur la complétude du ZW-calcul sur l'anneau des nombres complexes, la λ-box permettant notamment de rendre compte de la structure additive de l'anneau, non présente *a priori* dans le ZX-calcul.

ΔZX-calcul : un langage pour le fragment Toffoli+Hadamard

Renaud Vilmart a ensuite introduit le ΔZX-calcul, un langage intermédiaire entre le ZX-calcul standard et celui introduit par NG et Wang. Le ΔZX-calcul est une extension du ZX-calcul avec le triangle comme générateur. Ce langage est notamment approprié pour parler du fragment Toffoli+H de la mécanique quantique (Toffoli est la transformation unitaire sur 3 qubits qui transforme $|x, y, z\rangle$ et $|x, y, z + xy\rangle$). Il s'agit d'un fragment approximativement universel pour les matrices $2^n \times 2^m$ à coefficients réels.

II.2.2 Mécanique quantique pure à base de qutrits

Dans un ZX-diagramme, chaque fil représente un qubit, c'est à dire un sytème quantique à deux dimensions. Il est naturel de considérer des systèmes de dimension quelconque (finie). Harny Wang et Xiaoning Bian ont introduit une variante du ZX-calcul pour les systèmes de dimension 3 (*qutrits*) [16]. La principale différence est que la règle "seule la connectivité compte" ne s'applique malheureusement plus.

II.2.3 Mécanique quantique non pure

Il existe principalement deux constructions catégoriques permettant de représenter des évolutions quantiques non pures, i.e. des mesures (non post-selectionnées) ou des effacements de qubits par exemples. La première est la construction CPM introduite par Selinger [86]. Graphiquement, la construction CPM consiste essentiellement à doubler les diagrammes [31]. La seconde construction consiste à ajouter comme générateur le *discard* qui a pour effet d'effacer un qubit [33]. D'après la propriété de purification des évolutions quantiques [77], toute évolution quantique peut être décrite comme une évolution pure (isométrie) suivie de l'effacement d'une partie des qubits.

II.2.4 En dehors de la mécanique quantique

Il existe d'autres applications des langages graphiques, en dehors de la mécanique quantique, comme par exemple en théorie du contrôle [11], en algèbre linéaire [17], ou en traitement automatique des langues naturelles [66]. Il est intéressant de noter que l'un d'entre eux, le IH-calcul [17] partage (presque) la même syntaxe et les mêmes équations que le fragment sans angle du ZX-calcul. Le IH-calcul, introduit par Filippo Bonchi, Pawel Sobocinski, Fabio Zanasi, est un langage pour représenter les matrices. Le IH-calcul (pour *Interacting Hopf algebras*) a été introduit dans un contexte différent puisqu'il n'y a pas ici de motivations d'informatique ou de mécanique quantiques. Il s'agit d'un langage pour décrire des matrices de façon graphique. Contrairement au ZX-calcul où un diagramme à n entrées et m sorties représentent une matrice complexe de dimension $2^n \times 2^m$, un IH-diagramme représente une matrice de dimension $n \times m$.

Chapitre III

Des extensions nécessaires

Depuis l'introduction du ZX-calcul par Coecke et Duncan [28], le langage a évolué. Nous avons en particulier contribué à mettre en évidence de nouvelles équations, non démontrables à partir des équations originelles. Ces nouvelles équations font depuis partie du langage à part entière. Nous allons présenter dans ce chapitre ces différentes équations que nous avons montrées nécessaires.

Les résultats présentés ce chapitre s'appuient principalement sur les publications suivantes :

[10] Miriam Backens, Simon Perdrix, Quanlong (Harny) Wang. A Simplified Stabilizer ZX-calculus. QPL'17.

[39] Ross Duncan, Simon Perdrix. Graph States and the necessity of Euler Decomposition. CiE'09.

[40] Ross Duncan, Simon Perdrix. Rewriting measurement-based quantum computations with generalised flow. ICALP'10.

[64] Emmanuel Jeandel, Simon Perdrix, Renaud Vilmart, Quanlong (Harny) Wang. ZX-Calculus : Cyclotomic Supplementarity and Incompleteness for Clifford+T quantum mechanics. MFCS'17.

[78] Simon Perdrix, Quanlong (Harny) Wang. Supplementarity is Necessary for Quantum Diagram Reasoning. MFCS'16.

III.1 États Graphes et la décomposition d'Euler d'Hadamard

Dans cette section nous montrons comment les états graphes, un formalisme permettant de représenter des états quantiques en utilisant des graphes [53], peuvent être représentés et manipulés en ZX-calcul. Nous établissons un lien fort entre états

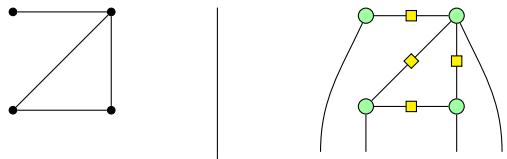
graphes et ZX-diagrammes, lien qui va nous permettre de mettre en évidence une équation non démontrable dans ZX_0.

III.1.1 États graphes en ZX-calcul

Le formalisme des états graphes (voir définition A.1.1) consiste à représenter certains états quantiques en utilisant un graphe simple non orienté : chaque sommet représente un qubit et les arêtes représentent intuitivement l'intrication entre ces qubits. Le formalisme des états graphes a de nombreuses applications en informatique quantique comme le calcul par mesure (MBQC [82, 35, 36]), le partage de secret quantique [72, 56], le calcul quantique à l'aveugle [20]...

Les états graphes ont une représentation très simple en ZX-calcul :

Propriété III.1.1. *Etant donné un graphe simple non orienté G d'ordre n, l'état graphe $|G\rangle$ est représenté par un ZX-diagramme où on associe à chaque sommet du graphe un nœud vert connecté à une sortie, et pour chaque arête du graphe, on connecte les nœuds correspondants via une boite Hadamard.*

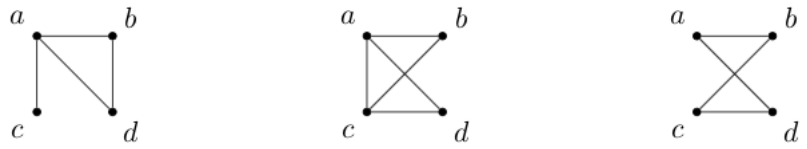


Graphe G | *ZX-diagramme pour $|G\rangle$*

La connexion entre état graphe et ZX-diagramme est profonde et fructueuse. On peut en effet représenter des calculs du modèle MBQC – qui consiste à effectuer un calcul en mesurant des qubits d'un état graphe – dans le formalisme du ZX-calcul de façon immédiate. Ainsi le ZX-calcul permet de représenter les circuits quantiques et le calcul par mesure qui sont de nature très différente dans un même formalisme. Nous avons montré avec Ross Duncan [40] qu'on peut alors utiliser la notion de *gflow* (voir section I.2.2) comme d'une stratégie permettant de transformer un calcul MBQC en le circuit correspondant. Les états graphes sont aussi au coeur de la preuve de complétude d'un fragment du ZX-calcul introduite par Miriam Backens [7] (voir section IV.1.1).

L'une des propriétés fondamentales des états graphes est qu'il existe une transformation graphique, la complémentation locale, qui ne modifie pas l'intrication de l'état quantique correspondant. La complémentation locale a été introduite par Kotzig [69], elle consiste, étant donné un sommet du graphe à complémenter le voisinage de ce sommet :

Définition III.1.2 (Complémentation Locale)**.** *Étant donné un graphe G et un sommet u de G, la complémentation locale de u dans G produit le graphe $G * u$ tel que $V(G * u) = V(G)$ et $E(G * u) = E(G)\Delta N_G(u) \times N_G(u)$, où $N_G(u)$ est le voisinage de u en G et Δ est la différence symétrique, i.e. $x \in A\Delta B$ ssi $x \in A$ xor $x \in B$.*



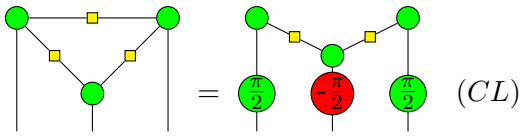
G $\quad$ $G \star a$ $\quad$ $(G \star a) \star b$

La complémentation locale peut être implémentée sur des états graphes à l'aide d'opérations locales :

Propriété III.1.3. *Pour tout G et tout u sommet de G,*

$$|G * u\rangle = \left(R_X^{(u)}(-\frac{\pi}{2}) \bigotimes_{v \in N_G(u)} R_Z^{(v)}(\frac{\pi}{2}) \right) |G\rangle$$

Dans le ZX-calcul une telle propriété correspond à l'équation suivante dans le cas où le graphe est un triangle :



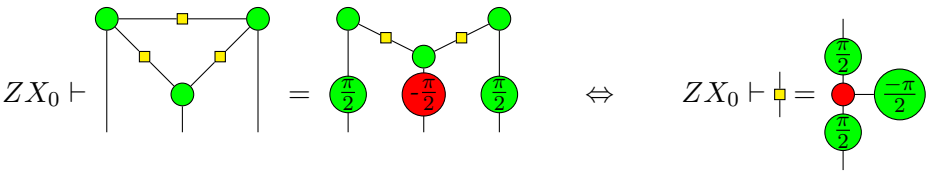
(CL)

Cette propriété est-elle démontrable en utilisant ZX_0 ? Une première propriété intéressante est que s'il existe une preuve en utilisant ZX_0 de l'équation précédente dans le cas particulier du triangle, alors il en existe une pour n'importe quel graphe.

III.1.2 Complémentation locale et décomposition d'Euler

Nous montrons dans un premier temps que l'équation (CL) est équivalente à une équation plus simple que l'on peut interpréter comme la décomposition d'Euler de la transformation d'Hadamard.

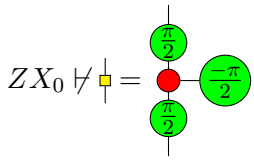
Propriété III.1.4.



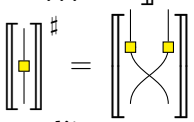
Cette équation plus simple peut être interprétée comme la décomposition d'Euler de H. En effet l'interprétation de est, à un scalaire non nul près, la même que celle de , ainsi H peut être décomposée en 3 rotations d'angle $\frac{\pi}{2}$.

Cette décomposition d'Euler de H ne peut pas être démontrable en utilisant ZX_0 :

Théorème III.1.5.



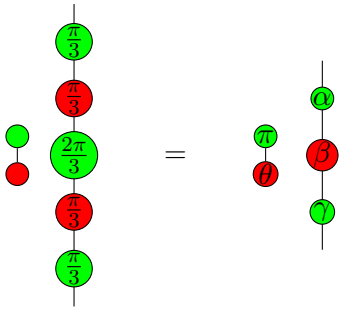
La preuve de ce théorème consiste à trouver une interprétation alternative des diagrammes du ZX-calcul pour laquelle toutes les équations du ZX_0-calcul II.1.3 sont vraies mais la décomposition d'Euler de Hadarmard ne l'est pas. Cette interprétation $[\![.]\!]^\sharp$ consiste à doubler tous les générateurs sauf , e.g.

Pour H auquel on ajoute un swap entre les deux copies.  . On peut vérifier facilement que toutes les équations de ZX_0 préservent l'interprétation alternative. En revanche la décomposition d'Euler ne préserve pas cette interprétation alternative, elle ne peut donc pas être dérivée à partir des règles de ZX_0.

III.1.3 ZX_H, une nouvelle théorie équationnelle

Dans la suite, nous noterons ZX_H la théorie équationnelle ZX_0 augmentée de l'équation de la décomposition d'Euler d'Hadamard. Bien que ZX_H soit strictement plus expressif que ZX_0, Christian Schröder de Witt et Vladimir Zamdzhiev ont démontré que le ZX_H-calcul n'est pas complet [85]. En effet, ils ont identifié une

équation, issue de la décomposition d'Euler d'une transformation unitaire particulière, telle que la transformation unitaire peut s'exprimer par un ZX-diagramme dont tous les angles sont des multiples rationnels de π, mais dont les angles d'Euler sont des multiples irrationnels de π :



Une telle équation n'est pas démontrable en utilisant ZX_H. Il suffit pour s'en convaincre de prendre une interprétation qui multiple par 3 les angles des diagrammes. Toutes les règles du ZX_H s'appliquent encore, en revanche l'équation précédente n'est pas correcte pour une telle interprétation. Schröder de Witt et Zamdzhiev n'ont pas proposé d'ajout de nouveaux axiomes au langage, car de multiples contre-exemples similaires peuvent être construits, sans pour autant dégager une règle simple à ajouter au langage.

Dans la suite de ce chapitre nous introduisons de nouvelles équations, mais comme nous le verrons, aucune d'entre elles ne permet d'atteindre la complétude du langage pour des angles arbitraires, la preuve d'incomplétude de Schröder de Witt et Zamdzhiev pouvant être adaptée aux nouveaux axiomes. Nous verrons dans le prochain chapitre IV que pour rendre le langage complet on peut soit considérer des fragments du langage qui ne contiennent pas d'angle multiple irrationnel de π, soit considérer des axiomes plus puissants permettant de transformer des angles multiples rationnels de π en des angles multiples irrationnels de π comme peut le faire par exemple une décomposition d'Euler.

III.2 L'axiomatisation des scalaires

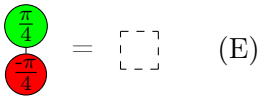
Alors que les scalaires ont été ignorés dans les premières versions du ZX-calcul, où les équations préservaient la sémantique des diagrammes à un scalaire près, la première axiomatisation des scalaires dans le ZX-calulus est due à Backens [7], que nous avons ensuite simplifiée avec Backens et Wang [10] :

La première équation indique simplement que le  est l'inverse du scalaire  , il s'agit simplement de l'équation $\sqrt{2}.\frac{1}{\sqrt{2}} = 1$.

L'interprétation de  est 0, en conséquence pour tous les diagrammes D_1 et D_2, $[\![\pi \otimes D_1]\!] = [\![\pi \otimes D_2]\!]$. Cette propriété d'absorption est capturée par la règle (ZO).

Définition III.2.1. *ZX_H augmenté de (IV) et (ZO) sera noté ZX_s.*

Avec Emmanuel Jeandel, Renaud Vilmart et Quanlong Wang [63], nous avons identifié une autre équation sur les scalaires qui ne peut pas être démontrée à partir des autres équations :



La preuve que l'équation (E) ne peut pas être dérivée des autres équations s'appuie sur un invariant graphique assez simple :

Définition III.2.2. *Étant donné un ZX-diagramme D, soit $[\![D]\!]$  (resp. $[\![D]\!]$ ) la parité du nombre de nœuds verts (resp. rouges) de degré impair plus le nombre de H dans D.*

Notez que pour tout scalaire $D : 0 \to 0$, $[\![D]\!]$  $+ [\![D]\!]$  $= 0 \bmod 2$, grâce à la formule bien connue qui implique que la somme des degrés des sommets d'un graphe est égale à deux fois le nombre d'arêtes. Plus généralement, pour tout $D : n \to m$, $[\![D]\!]$ $+ [\![D]\!]$ $= n + m \bmod 2$, qui est clairement un invariant du ZX-calcul puisque toutes les règles conservent le nombre d'entrées/sorties. En conséquence, une règle préserve $[\![.]\!]$ si et seulement si elle préserve $[\![.]\!]$.

On peut vérifier facilement que l'équation (E) ne préserve pas $[\![.]\!]$  . En revanche toutes les équations de ZX_H (sauf (ZO)) le préservent. Ceci est due à une propriété plus profonde du fragment $\frac{\pi}{2}$ des ZX-diagrammes, qui correspond au fragment stabilisable (ou Clifford) de la mécanique quantique :

Propriété III.2.3. *Pour toute paire de diagrammes D_1 et D_2 dans le fragment $\frac{\pi}{2}$, si $[\![D_1]\!] = [\![D_2]\!] \neq 0$ alors $[\![D_1]\!]$ $= [\![D_2]\!]$.*

Or, toutes les équations de ZX_s s'applique dans le fragment $\frac{\pi}{2}$ (au moins dans le cas où tous les angles sont nuls pour les équations paramétrées par des angles),

donc toutes ces équations doivent préserver l'invariant $[\![.]\!]_{\bullet}$. En conséquence, il y a nécessité d'avoir au moins une équation spécifique aux ZX-diagrammes qui ne sont pas dans le fragment $\frac{\pi}{2}$.

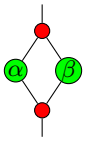
Nous noterons dans la suite ZX_E pour ZX_s augmenté de l'équation (E).

Définition III.2.4. *$ZX_E := ZX_s \cup (E)$*

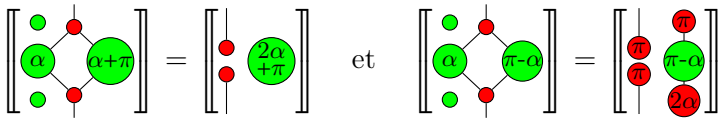
L'argument de Schröder de Witt et Zamdzhiev (voir section III.1.3) peut être adapté pour montrer que ZX_E n'est pas complet en général. L'argument ne s'applique plus dans le fragment $\frac{\pi}{4}$, mais nous montrons dans la prochaine section qu'il existe une propriété, la *supplémentarité*, mise en évidence par Coecke et Edwards qui n'est pas démontrable en utilisant ZX_E, même dans le fragment $\frac{\pi}{4}$.

III.3 Supplémentarité

Dans [29], Coecke et Edwards ont introduit la notion de *supplémentarité* en soulignant que lorsque $\alpha \neq 0 \bmod \pi$ l'interprétation standard du diagramme suivant est proportionnelle au projecteur $|0\rangle\langle 0|$ si $\alpha - \beta = \pi \bmod 2\pi$ et au projecteur $|1\rangle\langle 1|$ si $\alpha + \beta = \pi \bmod 2\pi$.



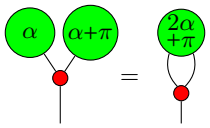
En replaçant les scalaires, on obtient les équations suivantes, qui sont vraies pour tout angle α, même lorsque $\alpha = 0$:



Coecke et Edwards ont montré que le concept de supplémentarité est lié à l'intrication des états quantiques. À opérations locales probabilistes et communications classiques (SLOCC) près, il n'y a que deux types d'états intriqués sur trois qubits : ceux qui sont SLOCC équivalents à un état $|GHZ\rangle = \frac{|000\rangle+|111\rangle}{\sqrt{2}}$, et ceux qui sont SLOCC équivalents à l'état $|W\rangle = \frac{|001\rangle+|010\rangle+|100\rangle}{\sqrt{3}}$. Un état GHZ est une instance particulière d'un état graphe qui peut facilement être représenté par un ZX-diagramme [39]. En revanche, il est moins aisé de représenter des états intriqués de type W. Le concept de supplémentarité a permis à Coecke et Edwards de caractériser les états de la classe W.

Ces équations sont-elles démontrables en utilisant le ZX-calcul ? Nous prouvons dans la section III.3.1 que ces équations peuvent être dérivées dans le ZX-calcul seulement quand $\alpha = 0 \bmod \frac{\pi}{2}$.

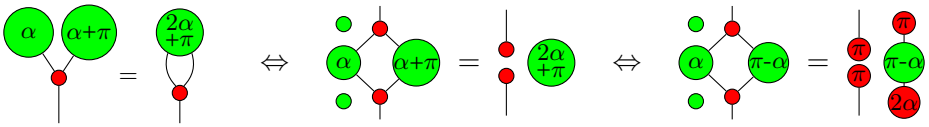
Inspirés par la propriété soulignée par Coecke et Edwards, nous introduisons l'équation suivante que nous appelons *supplémentarité* [78] :



(SUP)

La supplémentarité est correcte dans le sens où les deux diagrammes de l'équation (Eq. SUP) ont la même interprétation standard $\frac{1-e^{2i\alpha}}{\sqrt{2}}|0\rangle$. Elle est équivalente aux équations introduites par Coecke et Edwards :

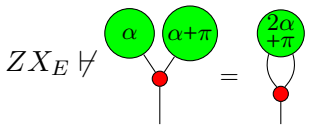
Lemme III.3.1. *Dans le ZX_E-calcul, pour tout $\alpha \in [0, 2\pi)$:*



III.3.1 La supplémentarité est nécessaire

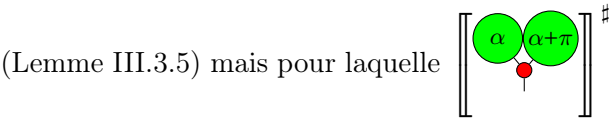
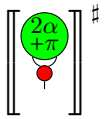
Dans cette section, nous montrons que la supplémentarité impliquant des angles qui ne sont pas des multiples de $\frac{\pi}{2}$ ne peut pas être dérivée en utilisant les règles du ZX-calcul, et comme corollaire que le fragment $\frac{\pi}{4}$ du ZX-calcul est incomplet.

Théorème III.3.2. *La supplémentarité ne peut pas être dérivée dans le ZX_E-calcul : pour tout $\alpha \neq 0 \bmod \frac{\pi}{2}$:*



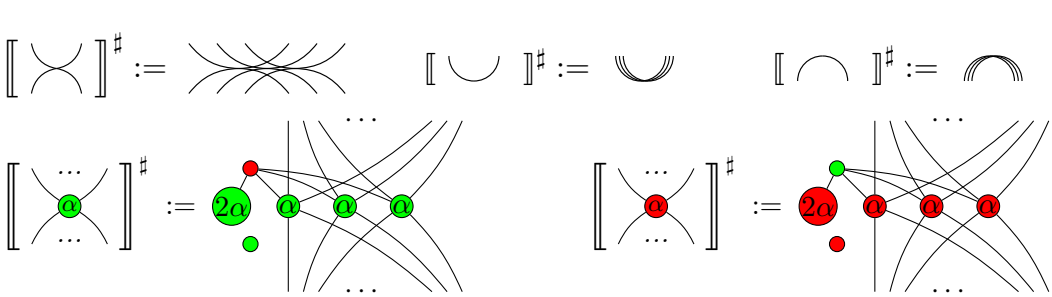
Corollaire III.3.3. *Le fragment du ZX_E-calcul $\frac{\pi}{4}$ n'est pas complet. En d'autres termes, le ZX_E-calcul n'est pas complet pour la mécanique quantique dite "Clifford+T".*

Le reste de la sous-section est dédiée à la preuve du Théorème III.3.2. Pour ce faire, nous introduisons une interprétation alternative $[\![.]\!]^\sharp$ pour les diagrammes,

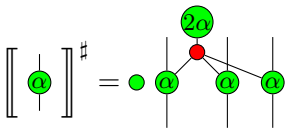
que nous prouvons être correcte (Lemme III.3.5) mais pour laquelle  $\neq$  quand $\alpha \neq 0 \bmod \frac{\pi}{2}$.

Définition III.3.4. *Pour tout diagramme $D : n \to m$, soit $[\![D]\!]^\sharp : 3n \to 3m$ un diagramme défini comme suit :*

$$[\![D_1 \otimes D_2]\!]^\sharp := [\![D_1]\!]^\sharp \otimes [\![D_2]\!]^\sharp \qquad [\![D_2 \circ D_1]\!]^\sharp := [\![D_2]\!]^\sharp \times [\![D_1]\!]^\sharp$$



Intuitivement, $[\![D]\!]^\sharp$ se compose de trois copies de D avec, pour chaque nœud d'angle α, un *gadget* paramétré par l'angle 2α reliant les trois copies du nœud. Par exemple,

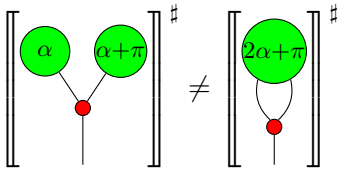


Des calculs simples montrent que le gadget disparaît lorsque $\alpha = 0 \bmod \pi$, par exemple :

Lemme III.3.5 (Correction)**.** $[\![.]\!]^\sharp$ *est une interprétation correcte : si $ZX_E \vdash D_1 = D_2$ alors $ZX_E \vdash [\![D_1]\!]^\sharp = [\![D_2]\!]^\sharp$.*

Pour terminer la preuve du Théorème III.3.2, il suffit de montrer que pour tout

$\alpha \neq 0 \bmod \frac{\pi}{2}$,



(III.1)

III.3.2 La supplémentarité comme axiome et interprétation graphique

Comme la supplémentarité ne peut dériver des autres règles du langage, nous proposons d'ajouter cette équation comme un axiome, une règle du ZX-calcul. Dans la suite nous noterons $\mathrm{ZX}_{\mathrm{supp}}$, les équations de ZX_E augmenté de la règle supplémentarité.

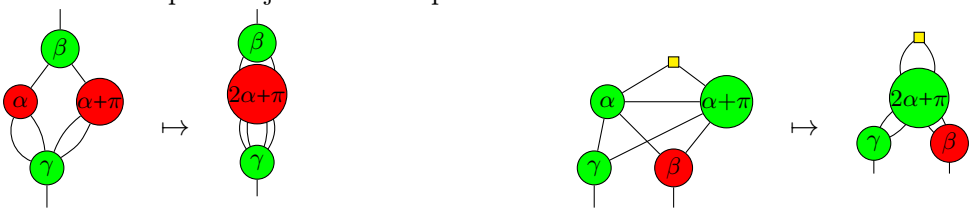
Définition III.3.6. *ZX_{supp} := $ZX_E \cup$ (SUP).*

Graphiquement, l'équation de supplémentarité (Eq. SUP) peut être interprétée comme la fusion de deux nœuds dans une configuration particulière : ils sont en opposition de phase (ou antiphasés, c'est-à-dire de même couleur et la différence entre les deux angles est π) ; de degré un ; et ils ont le même voisin. Alors que le fait d'être en opposition de phase est une condition nécessaire, les autres conditions peuvent être assouplies à n'importe quelle paire de nœuds "jumeaux" comme suit :

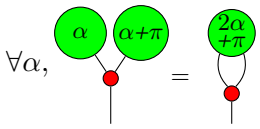
Définition III.3.7 (Jumeaux antiphasés)**.** *Deux nœuds u et v dans un ZX-diagramme sont jumeaux antiphasés si :*

- *ils sont de la même couleur ;*
- *la différence entre leurs angles est π ;*
- *ils ont le même voisinage : pour tout autre sommet ( ,  ou) w, le nombre de fils reliant u à w, et v à w sont les mêmes.*

Notez que les jumeaux antiphasés peuvent être directement connectés ou non. Voici deux exemples de jumeaux antiphasés et comment ils fusionnent :



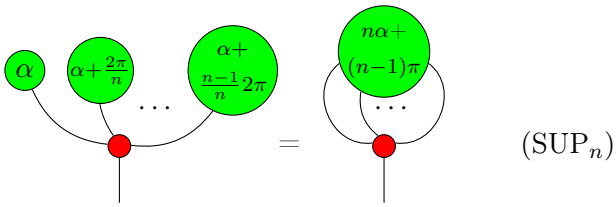
Théorème III.3.8 (Jumeaux antiphasés et supplémentarité)**.** *En ZX_E-calcul, n'importe quelle paire de jumeaux antiphasés peut être fusionnée si et seulement si*



Corollaire III.3.9. *En ZX_{supp}-calcul, n'importe quelle paire de jumeaux antiphasés peut être fusionnée*

III.3.3 Supplémentarité cyclotomique

Dans [64], nous avons généralisé le concept de supplémentarité comme suit : pour tout $n \in \mathbb{N}^*$, n nœuds partageant un même voisin peuvent être fusionnés lorsque leurs angles divisent le cercle en parties égales (cyclotomie), c'est-à-dire lorsque leurs angles sont de la forme $\alpha + \frac{2k\pi}{n}$ pour $k \in [\![0; n-1]\!]$:

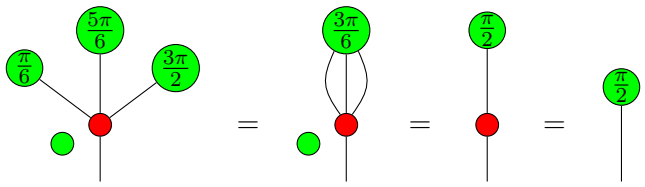


Notez qu'il y a n nœuds verts dans le diagramme de gauche et n fils parallèles dans celui de droite.

Chacune de ces équations est valable pour l'interprétation standard des ZX-diagrammes :

Proposition III.3.10. (SUP$_n$) *est correcte.*

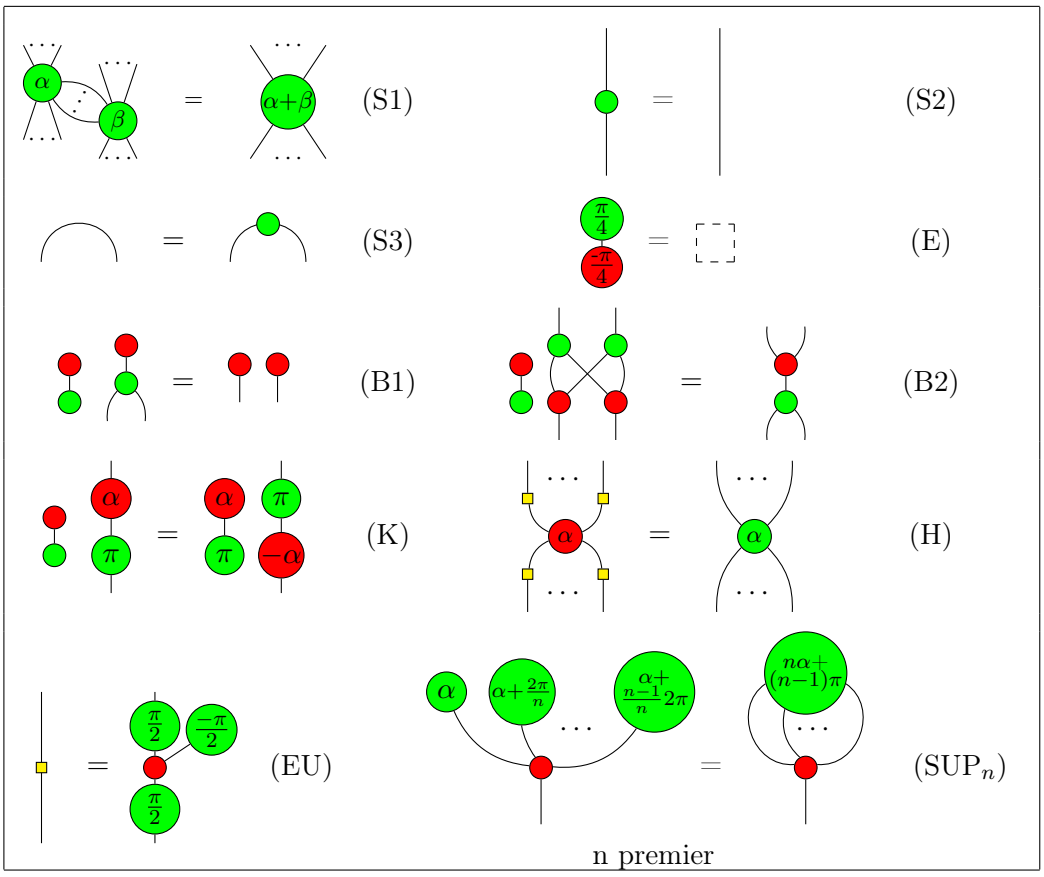
La supplémentarité cyclotomique permet de mettre en évidence des propriétés spécifiques à des angles qui ne sont pas des multiples de $\frac{\pi}{4}$. En effet tous les autres règles du ZX-calculus sont soit valables pour des angles arbitraires, soit spécifiques aux multiples de $\frac{\pi}{4}$. On peut ici parler d'équations qui sont spécifiques aux multiples de $\frac{\pi}{6}$ par exemple :



La règle (SUP_n) est de nature très différente suivant la parité de n, en effet grace à loi de Hopf II.1 si n est pair alors tous les fils entre les nœuds vert et rouge disparaissent, alors qu'il en reste un quand n est impair. Une autre propriété interessante est que si $n = pq$ n'est pas premier, alors on peut facilement démontrer (SUP_n) en utilisant (SUP_p) et (SUP_q). *A contrario*, pour chaque p premier impair il n'est pas possible de prouver SUP_p à partir des autres autres suppléméntarités cyclotomiques $\{\mathrm{SUP}_q\}_{q \text{ premier, différent de } p}$.

On en déduit une nouvelle axiomatisation $\mathrm{ZX}_{\mathrm{cyclo}}$ du ZX-calcul.

Définition III.3.11. *$ZX_{\mathrm{cyclo}} := ZX_{\mathrm{supp}} \cup \{(\mathrm{SUP}_n)\}_{n \text{ premier}}$*



Bien que la supplémentarité cyclotomique permette de capturer de nouvelle propriétés, le nouveau calcul $\mathrm{ZX}_{\mathrm{cyclo}}$ n'est pas complet pour autant, l'argument de Schröder de Witt et Zamdzhiev (voir section III.1.3) pouvant être adapté.

Interprétation graphique de la supplémentarité cyclotomique

Tout comme la supplémentarité, la supplémentarité cyclotomique a une généralisation : les nœuds verts peuvent être fusionnés non seulement lorsqu'ils partagent un même voisin, mais aussi lorsqu'ils partagent le même voisinage. Elle conduit à la notion de jumeaux cyclotomiques, qui généralisent la notion de jumeaux antiphasés :

Définition III.3.12 (Jumeaux Cyclotomiques)**.** *Un ensemble de n nœuds dans un ZX-diagramme sont des jumeaux cyclotomiques si :*

- *ils ont la même couleur*
- *leurs angles divisent le cercle en parties égales $\left(\alpha + \frac{2k\pi}{n} \text{ for } k \in [\![0; n-1]\!]\right)$*
- *ils ont le même voisinage : pour chaque sommet, le nombre de fils qui le relient à l'un des jumeaux est le même.*

Proposition III.3.13 (Jumeaux Cyclotomiques et Supplémentarité)**.** *Avec ZX_{cyclo}, les jumeaux cyclotomiques peuvent être fusionnés.*

Chapitre IV

Complétude(s)

Dans le chapitre précédent nous avons identifié des équations qui ne peuvent pas être dérivées en utilisant les autres équations du langage. Nous abordons dans ce chapitre la question de la complétude du langage : un ensemble d'équations est complet si pour toute paire de diagrammes D_1, D_2 tels que $[\![D_1]\!] = [\![D_2]\!]$ alors D_1 peut être transformé en D_2 en utilisant les équations du langage.

Nous allons présenter ici plusieurs résultats de complétudes, correspondant à différents fragments (ou variantes) du ZX-calcul. Nous allons présenter rapidement le premier résultat de complétude, obtenu par Miriam Backens, du ZX-calcul pour le fragment $\frac{\pi}{2}$ du ZX-calcul, ainsi que le résultat de complétude obtenu par Hadzihasanovic du ZW-calcul, un langage cousin du ZX-calcul qui permet de représenter des matrices entières. Nous allons ensuite présenter l'un des résultats principaux de ce manuscript, la complétion du ZX-calcul pour le fragment $\frac{\pi}{4}$, i.e. le fragment Clifford+T de la mécanique quantique. Il s'agit du premier résultat de complétude pour un fragment (approximativement) universel de la mécanique quantique. Une extension de notre résultat de complétude au ZX-calcul (sans restriction sur les angles) a été introduit par Ng et Wang. Enfin nous présentons des formes normales génériques qui permettent de montrer la complétude (voire de compléter) les fragments du langage qui contiennent au moins le fragment $\frac{\pi}{4}$. En utilisant ces formes normales génériques, nous présenterons une axiomatisation plus simple que celle de Ng et Wang pour le ZX-calcul sans restriction.

Il existe donc plusieurs résultats de complétude pour le ZX-calcul, suivant le fragment considéré. À titre de comparaison, le formalisme des circuits quantiques ne bénéficie pas de théorie équationnelle complète pour un fragment universel. Il existe différentes théories équationnelles qui ont été montrées complètes pour des fragments non universel des circuits quantiques : le fragment Clifford [87], le fragment CNot dihédral (circuits dont les portes sont CNot, X ou T) [4], Clifford+T sur

1 qubit [74], ou sur au plus deux qubits [88]. Aucune théorie équationnelle pour un fragment universel des circuits quantiques n'est connue à ce jour.

Les résultats présentés ce chapitre s'appuient principalement sur les publications suivantes :

[41] Ross Duncan, Simon Perdrix. Pivoting makes the ZX-calculus complete for real stabilizers. QPL'13.

[60] Emmanuel Jeandel, Simon Perdrix, Renaud Vilmart. A Complete Axiomatisation of the ZX-Calculus for Clifford+T Quantum Mechanics, LiCS'18.

[61] Emmanuel Jeandel, Simon Perdrix, Renaud Vilmart. Diagrammatic Reasoning beyond Clifford+T Quantum Mechanics, LiCS'18.

[62] Emmanuel Jeandel, Simon Perdrix, Renaud Vilmart. A generic normal form for ZX-diagrams and application to the rational angle completeness. *arXiv 1805.05296*.

IV.1 Complétude pour des fragments non universels

IV.1.1 Fragment $\pi/2$: la mécanique quantique stabilisable

Miriam Backens a démontré la complétude du ZX_s-calcul pour le fragment $\frac{\pi}{2}$ du langage, correspondant à la mécanique quantique stabilisable (aussi appelée Clifford) [7]. Pour ce faire, elle a montré que tout diagramme peut être transformé en un diagramme représentant un état graphe, à des opérations locales simples près. Cette représentation n'est pas unique, mais elle a montré que l'on peut passer d'une telle forme pseudo-normale à une autre en utilisant les équations du langage.

IV.1.2 Fragment π : la mécanique quantique stabilisable réelle

Avec Ross Duncan nous avons introduit une théorie équationnelle complète pour le fragment π du langage [41]. Ce fragment correspond à restriction réelle du fragment stabilisable de la mécanique quantique. La preuve de complétude s'appuie également sur l'utilisation des états graphes, comme la preuve de Backens pour le fragment $\frac{\pi}{2}$. À noter que Vilmart a introduit le Y-calcul, une extension de ce langage à toute la mécanique quantique réelle [59].

IV.1.3 Diagrammes de chemins du fragment $\frac{\pi}{4}$

Miriam Backens a également prouvé un résultat de complétude pour les diagrammes de chemins du fragment $\frac{\pi}{4}$ [8], il s'agit de ZX-diagrammes avec une entrée

et une sortie pour lesquels il existe un unique chemin de l'entrée vers la sortie, et dont les angles sont des multiples de $\frac{\pi}{4}$.

IV.1.4 Le ZW-calcul pour les matrices à coefficients entiers

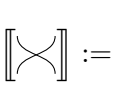
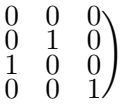
Le ZW-calcul a été introduit par Amar Hadzihasanovic [50], il s'agit d'une variante du ZX-calcul s'appuyant sur l'axiomatisation des états GHZ/W introduite par Coecke et Kissinger [30]. Bien que le langage trouve racine dans l'axiomatisation catégorique de la mécanique quantique, une spécificité importante de ce langage est qu'il ne permet de représenter que des matrices à coefficients entiers. Hadzihasanovic a démontré la complétude de ce langage en introduisant une notion de forme normale pour les ZW-diagrammes. Bien que ce langage ne soit pas universel, dans le sens où il ne permet pas de représenter, ou même d'approximer toute évolution quantique, ce résultat de complétude joue un rôle important dans la preuve de complétude du ZX-calcul que nous avons introduite (voir section IV.2.1). À noter que Hadzihasanovic, Ng et Wang ont introduit récemment le $\mathrm{ZW}_{\mathbb{C}}$-calcul une extension du ZW-calcul aux matrices à coefficients complexes, qui est également complète [52].

Syntaxe et sémantique

Comme pour le ZX-calcul, nous définissons une interprétation standard, qui associe à n'importe quel diagramme D du ZW-calcul avec n entrées et m sorties m, une application linéaire $[\![D]\!] : \mathbb{Z}^{2^n} \mapsto \mathbb{Z}2^m$, définie inductivement comme :

$[\![.]\!]$

$$[\![D_1 \otimes D_2]\!] := [\![D_1]\!] \otimes [\![D_2]\!] \qquad [\![D_2 \circ D_1]\!] := [\![D_2]\!] \circ [\![D_1]\!]$$


$:= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

$:= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$


$:= (1)$ 
$:= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $[\![\cup]\!] := (1 \quad 0 \quad 0 \quad 1)$


$:= \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$
$:= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ 
$:= \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 0 \end{pmatrix}$

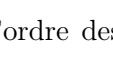

$:= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ 
$:= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$

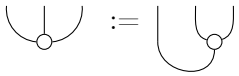
L'interprétation $[\![.]\!]$ est évidemment différente de celle du ZX-calcul – le domaine est différent – mais nous utiliserons la même notation.

Lemme IV.1.1 ([50])**.** *Les ZW-Diagrammes sont universels pour les matrices entières.*

$$\forall A \in \mathbb{Z}^{2^n} \times \mathbb{Z}^{2^m}, \quad \exists D : n \to m, \quad [\![D]\!] = A$$

Les règles du langage

Le ZW-calcul est équipé d'un ensemble de règles qui est donné dans la figure IV.1. Ici comme pour le ZX-calcul, le paradigme *seule la connectivité compte* s'applique sauf pour  où l'ordre des entrées et sorties est important $\left(\right.$  $\left.\right)$. Ce paradigme donne un sens aux nœuds qui ne sont pas directement donnés dans la syntaxe, par exemple :



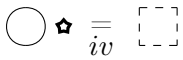
Toutes ces règles sont correctes, elles préservent la sémantique des diagrammes. Nous utilisons la même notation $\vdash$ que celle définie dans la section II.1, et nous pouvons toujours appliquer les règles de réécriture aux sous-diagrammes. Dans ce qui suit, nous utiliserons les raccourcis :

Théorème IV.1.2 (Complétude [51])**.** *Le ZW-calcul est complet : pour toute paire $D_1, D_2 : n \to m$ de ZW-diagrammes, si $[\![D_1]\!] = [\![D_2]\!]$ alors $ZW \vdash D_1 = D_2$.*

IV.1.5 Extension du ZW-calcul aux matrices dyadiques

Dans [60], nous avons montré que le ZW-calcul peut être rendu plus expressif, pour représenter toute matrice à coefficients dyadiques, i.e. coefficient de la forme $\frac{p}{2^n}$, avec $p, n \in \mathbb{Z}$. Cette extension est relativement simple, elle ne nécessite qu'un nouveau symbole (pour représenter le scalaire $\frac{1}{2}$) et une nouvelle règle pour obtenir un langage complet.

Nous définissons le $\mathrm{ZW}_{1/2}$-calcul comme une extension du ZW-calcul avec le nouveau symbole ✿ et l'équation suivante :



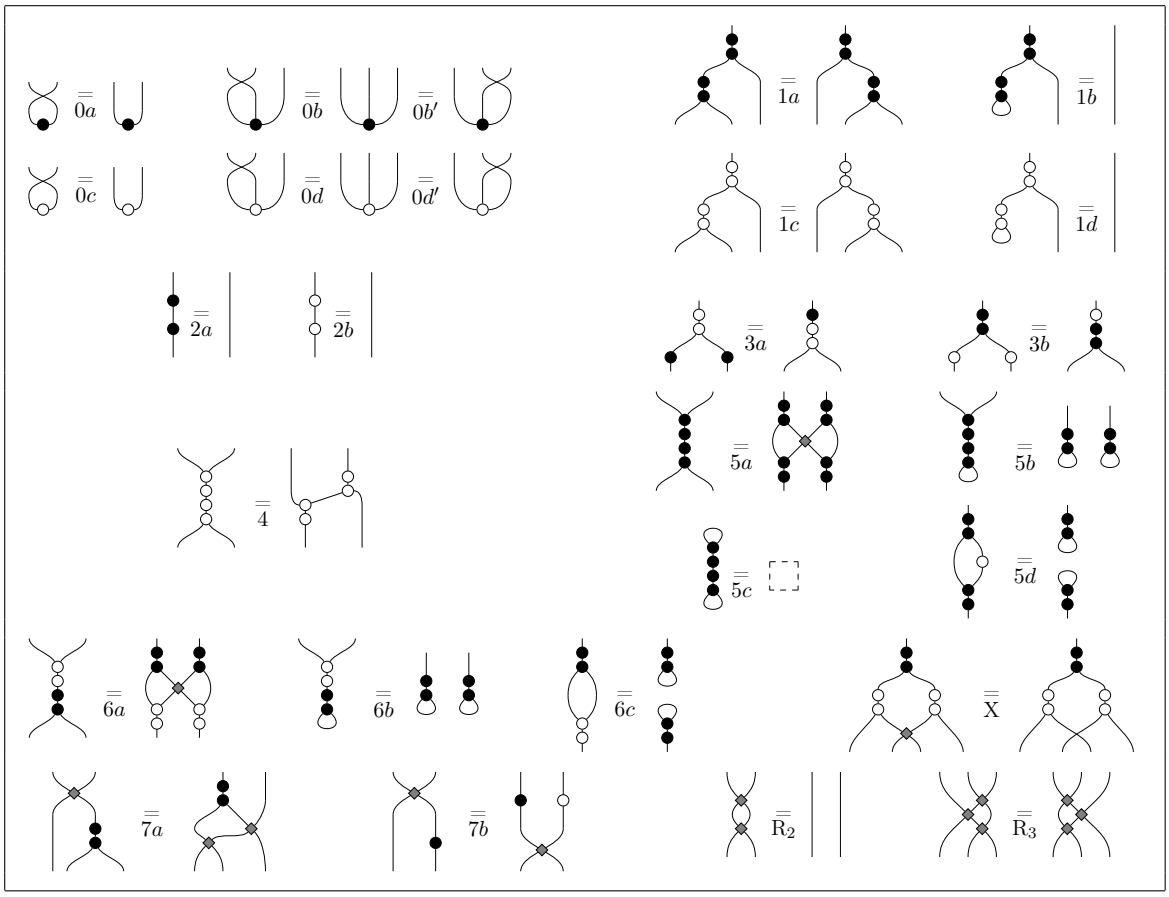


FIGURE IV.1 – Règles du ZW-calcul.

L'interprétation standard d'un $\mathrm{ZW}_{1/2}$-diagramme $D : n \to m$ est une matrice $[\![D]\!] : \mathbb{D}^{2^n} \to \mathbb{D}^{2^m}$ sur l'anneau $\mathbb{D} = \mathbb{Z}[1/2]$ des rationnels dyadiques et est donné par la sémantique standard du ZW-calcul étendue avec $[\![\text{✿}]\!] := \left(\frac{1}{2}\right)$.

Proposition IV.1.3. *Le* $\mathrm{ZW}_{1/2}$*-calcul est correct et complet : pour toute paire* D_1, D_2 *de diagrammes du* $\mathrm{ZW}_{1/2}$*-calcul,* $[\![D_1]\!] = [\![D_2]\!]$ *ssi* $\mathrm{ZW}_{1/2} \vdash D_1 = D_2$.

IV.2 Fragments (approximativement) universels

IV.2.1 Fragment $\pi/4$ du ZX-calcul

Dans cette section nous considérons le plus simple fragment universel du ZX-calcul : le fragment $\pi/4$ de tous les diagrammes dont les angles sont des multiples de

$\pi/4$. Ce fragment correspond au fragment Clifford+T de la mécanique quantique : peut être représentée dans le fragment $\pi/4$, toute évolution obtenue par initialisation de qubits à $|0\rangle$, application de transformations unitaires H, T et ΛX suivi de mesures post-sélectionnées dans la base standard. En terme de matrices le fragment $\pi/4$ est universel pour les matrices à coefficients dans $\mathbb{Z}[\frac{1}{\sqrt{2}}, i]$ le plus petit sous anneau de $\mathbb{C}$ contenant $\mathbb{Z}, \frac{1}{\sqrt{2}}$ et i. A noter que $\mathbb{Z}[\frac{1}{\sqrt{2}}, i] = \mathbb{D}[e^{i\frac{\pi}{4}}] = \{a + be^{i\frac{\pi}{4}} + ce^{i\frac{\pi}{2}} + de^{i\frac{3\pi}{4}} \mid a, b, c, d \in \mathbb{D}\}$, une extension des nombres dyadiques.

Proposition IV.2.1. *Le fragment $\frac{\pi}{4}$ du ZX-calcul représente exactement les matrices sur $\mathbb{D}[e^{i\frac{\pi}{4}}]$:*

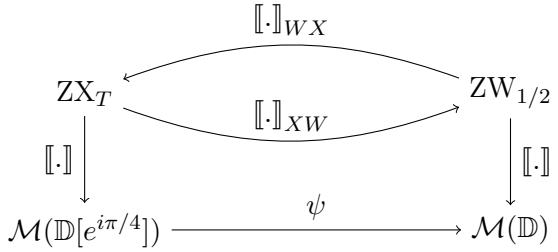
- *pour tout ZX-diagramme $D : n \to m$ dans le fragment $\frac{\pi}{4}$, $[\![D]\!] \in \mathbb{D}[e^{i\frac{\pi}{4}}]^{2^n \times 2^m}$*
- *$\forall A \in \mathbb{D}[e^{i\frac{\pi}{4}}]^{2^n \times 2^m}$, il existe un ZX-diagramme $D : n \to m$ dans le fragment $\frac{\pi}{4}$ tel que $[\![D]\!] = A$.*

Le principal résultat de cette section est la preuve de complétude du ZX-calcul pour le fragment Clifford+T de la mécanique quantique. En effet les axiomes donnés dans la figure IV.2 sont complets.

Définition IV.2.2. *On notera ZX_T les axiomes de la figure IV.2.*

Théorème IV.2.3. *Le fragment $\frac{\pi}{4}$ du ZX-calcul dont les axiomes sont donnés en Figure IV.2 est complet : pour toute paire de diagrammes dans le fragment $\pi/4$ du ZX-calcul, $[\![D_1]\!] = [\![D_2]\!]$ ssi $\mathrm{ZX}_T \vdash D_1 = D_2$.*

La preuve consiste en une double traduction entre le ZX_T et le $\mathrm{ZW}_{1/2}$, qui permet intuitivement de transférer le résultat de complétude $\mathrm{ZW}_{1/2}$ au fragment $\frac{\pi}{4}$ de ZX_T.



Les traductions $[\![.]\!]_{WX}$ et $[\![.]\!]_{XW}$ sont décrites en Figures IV.3 et IV.4.
L'interprétation $[\![\cdot]\!]_{WX}$ préserve la sémantique et la prouvabilité :

Proposition IV.2.4. *Soient D_1, D_2 deux diagrammes du $\mathrm{ZW}_{1/2}$-calcul.*
Si $\mathrm{ZW}_{1/2} \vdash D_1 = D_2$ alors $\mathrm{ZX}_T \vdash [\![D_1]\!]_{WX} = [\![D_2]\!]_{WX}$

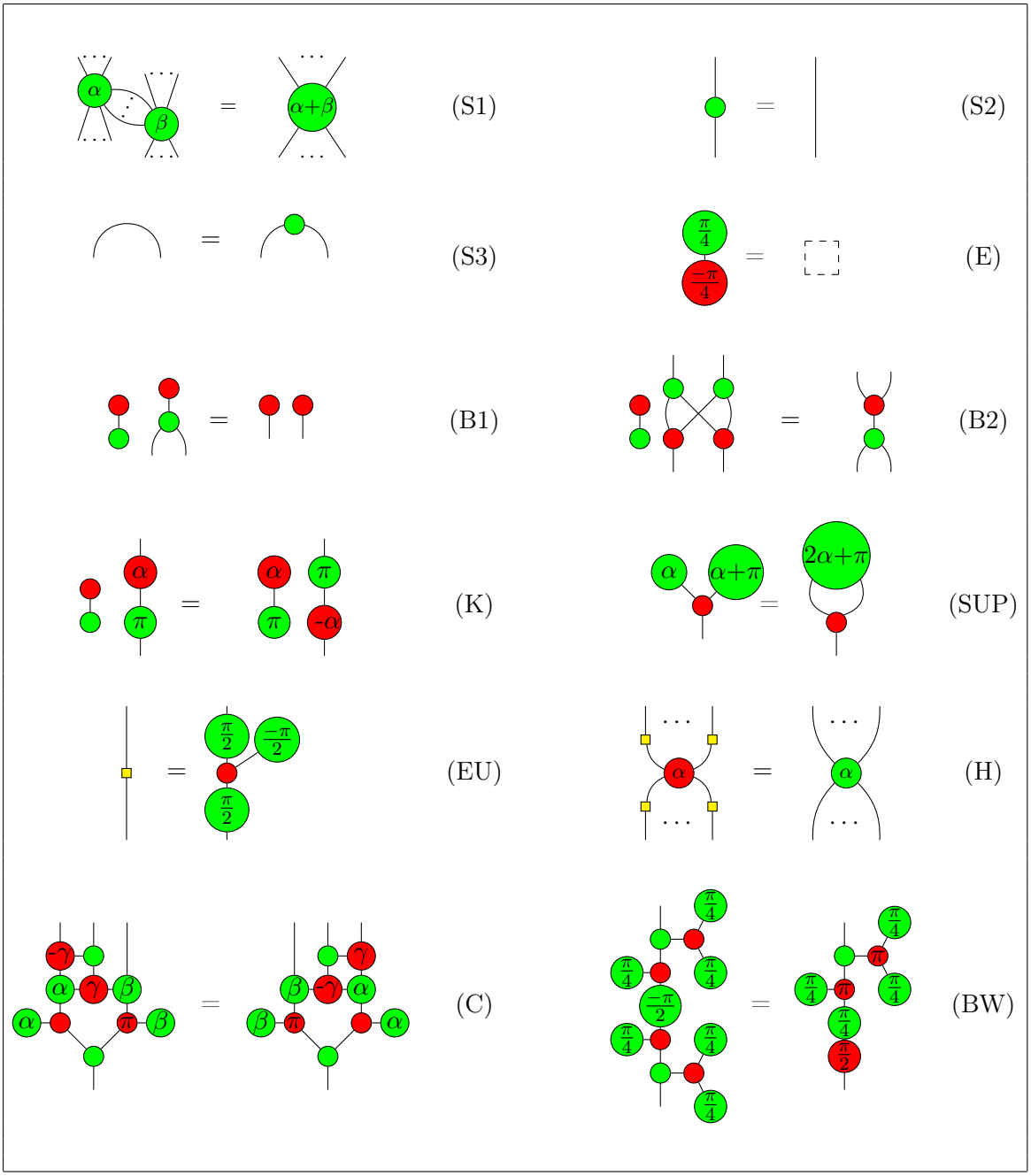


FIGURE IV.2 – Ensemble des règles pour le ZX_T-calcul. Toutes ces règles s'appliquent également lorsque les couleurs rouge et vert sont permutées. Le côté droit de (E) est un diagramme vide. (...) indiquent zéro fil ou plus, tandis que (.˙.) indiquent un ou plusieurs fils.

En ce qui concerne la traduction du fragment $\frac{\pi}{4}$ du ZX_T vers $\mathrm{ZW}_{1/2}$, elle ne peut pas préserver la sémantique car les diagrammes du fragment $\frac{\pi}{4}$ de ZX_Treprésentent des matrices de $\mathcal{M}(\mathbb{D}[e^{i\pi/4}])$ alors que les $\mathrm{ZW}_{1/2}$-diagrammes représentent des matrices à coefficients dyadiques. Un encodage est nécessaire. Intuitivement $\mathbb{D}[e^{i\pi/4}]$ est un $\mathbb{D}$ module de dimension 4, donc on peut encoder chaque élément de $\mathbb{D}[e^{i\pi/4}]$ comme une matrice 4×4 à coefficients dyadiques. Cet encodage est donné par la fonction $\psi : A + Be^{i\frac{\pi}{4}} + C(e^{i\frac{\pi}{4}})^2 + D(e^{i\frac{\pi}{4}})^3 \mapsto A \otimes I_4 + B \otimes M + C \otimes M^2 + D \otimes M^3$ avec $M = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \end{pmatrix}$.

Proposition IV.2.5. *Soit D un ZX-diagramme dans fragment $\frac{\pi}{4}$,*

$$[\![[\![D]\!]_{XW}]\!] = \psi([\![D]\!])$$

La composition des deux interprétations ne permet pas de reproduire le diagramme initial à cause de l'encodage, on obtient en fin de compte un diagramme avec deux entrées supplémentaires. Cependant,

Proposition IV.2.6. *Soient D_1, D_2 des diagrammes du fragment $\frac{\pi}{4}$ du ZX-calcul, si $\mathrm{ZX}_T \vdash [\![[\![D_1]\!]_{XW}]\!]_{WX} = [\![[\![D_2]\!]_{XW}]\!]_{WX}$ alors $\mathrm{ZX}_T \vdash D_1 = D_2$.*

On peut en déduire maintenant notre théorème principal :

Preuve du théorème IV.2.3. Soient D_1, D_2 deux diagrammes du fragment $\frac{\pi}{4}$ du ZX_T-calcul tels que $[\![D_1]\!] = [\![D_2]\!]$. On a $[\![[\![D_1]\!]_{XW}]\!] = [\![[\![D_2]\!]_{XW}]\!]$. De plus par complétude du $\mathrm{ZW}_{1/2}$-calcul $\mathrm{ZW}_{1/2} \vdash [\![D_1]\!]_{XW} = [\![D_2]\!]_{XW}$. D'après la Proposition IV.2.4, $\mathrm{ZX}_T \vdash [\![[\![D_1]\!]_{XW}]\!]_{WX} = [\![[\![D_2]\!]_{XW}]\!]_{WX}$, donc, grâce à la proposition IV.2.6, cela implique $\mathrm{ZX}_T \vdash D_1 = D_2$. □

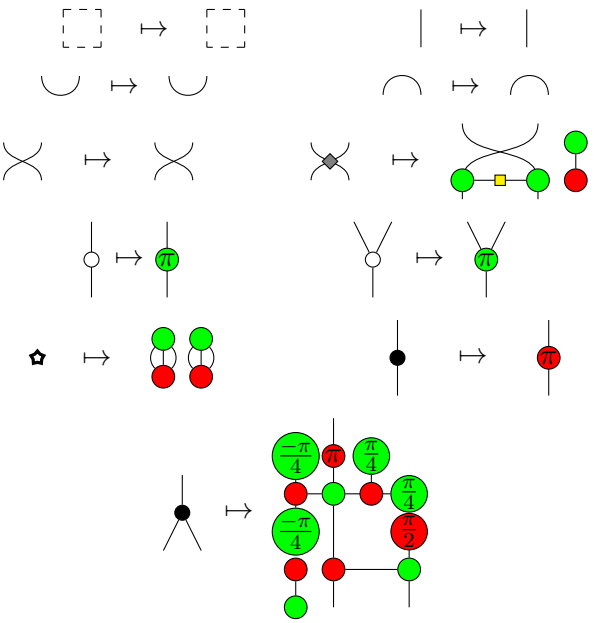
Cette approche donne une procédure de complétion. Il donne un ensemble d'égalités entre les ZX_T-diagrammes dont la dérivabilité prouve la complétude du langage. Par conséquent, les nouvelles règles du ZX_T-calcul que nous avons introduites ont évidemment été choisies pour que les propositions IV.2.6 et IV.2.4 soient satisfaites. Cependant, un travail important a été de simplifier ces règles par rapport à ce que l'on peut obtenir en utilisant cette approche de manière naïve.

IV.2.2 Au-delà de Clifford+T

Variables et Constantes

Il est d'usage de considérer certains angles dans les ZX-diagrammes comme des variables, afin de prouver des familles d'égalité. Par exemple, la règle (S1) possède

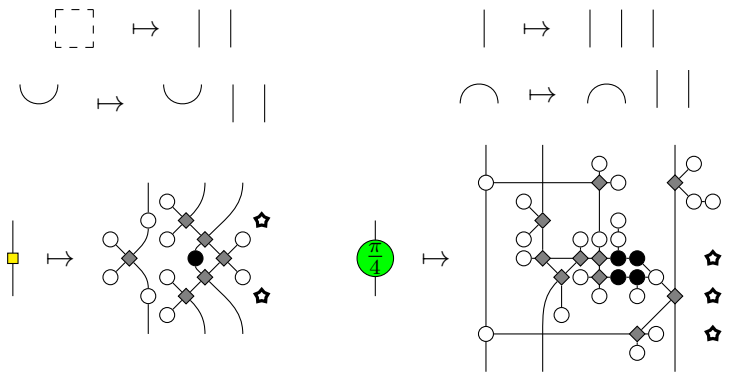
$[\![.]\!]_{WX}$



$$D_1 \circ D_2 \mapsto [\![D_1]\!]_{WX} \circ [\![D_2]\!]_{WX}$$
$$D_1 \otimes D_2 \mapsto [\![D_1]\!]_{WX} \otimes [\![D_2]\!]_{WX}$$

FIGURE IV.3 –

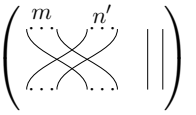
$[\![.]\!]_{XW}$



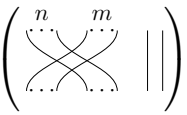
$\forall D_1 : n \to n',\ \forall D_2 : m \to m' :$

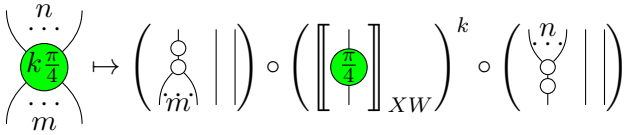
$$D_1 \circ D_2 \mapsto [\![D_1]\!]_{XW} \circ [\![D_2]\!]_{XW} \qquad (\text{if } m' = n)$$

$$D_1 \otimes D_2 \mapsto \left(\mathbb{I}^{\otimes n'} \otimes [\![D_2]\!]_{XW}\right) \circ$$



$$\circ \left(\mathbb{I}^{\otimes m} \otimes [\![D_1]\!]_{XW}\right) \circ$$





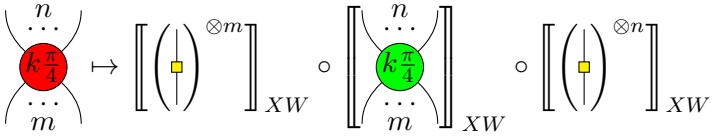
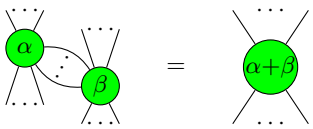


Figure IV.4 –

deux variables α et β, et donne potentiellement un nombre infini d'égalités :



On peut remarquer que dans les axiomes du ZX-calcul, les opérations sur les angles sont assez restreintes, il s'agit d'opérations d'addition d'angles, avec des constantes qui sont des multiples rationnels de π, et plus précisément des multiples de $\frac{\pi}{4}$ dans le cas de ZX_T. L'addition est celle du groupe $\mathbb{R}/2\pi\mathbb{Z}$ des angles (appelé *phase group* [28]). Ainsi les variables sont utilisées de manière linéaire, dans le sens suivant :

Définition IV.2.7. *Un ZX-diagramme est linéaire en $\alpha_1, \ldots, \alpha_k$ avec des constantes dans $C \subseteq \mathbb{R}$, s'il est généré par $R_Z^{(n,m)}(E)$, $R_X^{(n,m)}(E)$, H, e, $\mathbb{I}$, sigma, ϵ, η, et les compositions spatiales et séquentielles, où $n, m \in \mathbb{N}$, et E est de la forme $\sum_i n_i\alpha_i + c$, avec $n_i \in \mathbb{Z}$ et $c \in C$.*

Tous les diagrammes de la Figure IV.2 sont linéaires en α, β, γ avec constantes dans $\frac{\pi}{4}\mathbb{Z}$. Un diagramme linéaire en $\alpha_1, \ldots, \alpha_k$ est noté $D(\alpha_1, \ldots, \alpha_k)$, ou $D(\vec{\alpha})$ avec $\vec{\alpha} = \alpha_1, \ldots, \alpha_k$. Evidemment, si $D(\alpha)$ est un diagramme linéaire en α, $D(\pi/2)$ désigne le ZX-diagramme où toutes les occurrences de α sont remplacées par $\pi/2$.

Alors que l'ensemble des règles de la Figure IV.2 est complet pour le fragment Clifford+T de la mécanique quantique, on peut aussi prouver beaucoup d'égalités au-delà de ce fragment, quand on considère les règles (S1), (H), (K), (K), (C) avec des angles arbitraires, plutôt que des angles multiples de $\frac{\pi}{4}$.

En fait, on peut prouver toutes les égalités qui sont valides pour les diagrammes linéaires avec des constantes dans $\frac{\pi}{4}\mathbb{Z}$, dans le sens suivant :

Théorème IV.2.8. *Pour toute paire $D_1(\vec{\alpha})$ et $D_2(\vec{\alpha})$ de ZX-diagrammes linéaires en $\vec{\alpha} = \alpha_1, \ldots, \alpha_k$ avec constante dans $\frac{\pi}{4}\mathbb{Z}$,*

$$\forall \vec{\alpha} \in \mathbb{R}^k, [\![D_1(\vec{\alpha})]\!] = [\![D_2(\vec{\alpha})]\!] \;\Leftrightarrow\; \forall \vec{\alpha} \in \mathbb{R}^k, \mathrm{ZX}_T \vdash D_1(\vec{\alpha}) = D_2(\vec{\alpha})$$

Autrement dit, les équations qui ne sont pas prouvables en ZX-calcul sont des propriétés qui sont spécifiques à des angles particuliers, non multiples de $\frac{\pi}{4}$.

Le théorème IV.2.8 est puissant et démontre que le ZX_T-calcul est très expressif, au delà du fragment $\frac{\pi}{4}$, en revanche l'application en pratique de ce théorème peut être problématique à cause du quantificateur universel sur les angles. Nous considérons ci-dessous trois cas où le théorème IV.2.8 peut être utilisé en pratique.

Cas 1 – Examen d'une base

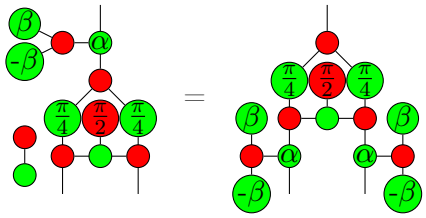
Théorème IV.2.9. *Pour toute paire de ZX-diagramme* $D_1(\vec{\alpha}), D_2(\vec{\alpha}) : 1 \to m$ *linéaires en* $\vec{\alpha} = \alpha_1, \ldots, \alpha_k$ *avec constante dans* $\frac{\pi}{4}\mathbb{Z}$*, si*

$$\forall j \in \{0,1\}, \forall \vec{\alpha} \in \mathbb{R}^k, \mathrm{ZX} \vdash D_1(\vec{\alpha}) \circ R_X(j\pi) = D_2(\vec{\alpha}) \circ R_X(j\pi)$$

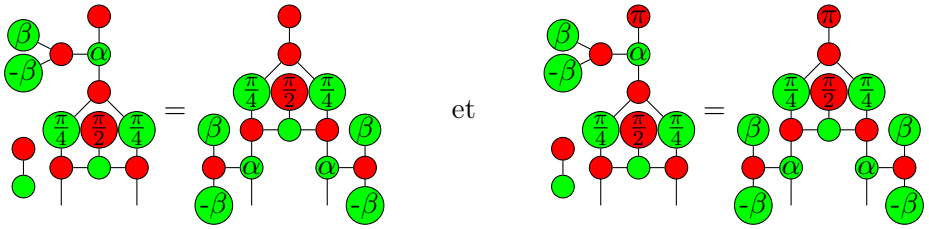
alors

$$\forall \vec{\alpha} \in \mathbb{R}^k, \mathrm{ZX}_T \vdash D_1(\vec{\alpha}) = D_2(\vec{\alpha})$$

On peut condidérer par exemple l'équation suivante :

$\forall \alpha, \beta \in \mathbb{R}, \mathrm{ZX}_T \vdash$ 

Cette équation peut s'interpréter comme la 'copie' du sous diagramme dépendant de α et β par le sous diagramme dont les angles sont des multiples de $\frac{\pi}{4}$. Une preuve directe de cette équation n'est pas évidente. En revanche, en utilisant le théorème IV.2.9, il suffit de prouver cette équation pour la base $\left(\; , \; \right)$, et donc de faire deux preuves indépendantes qui sont plus faciles à mener :



(voir Annexe A.4 dans [61] pour une preuve détaillée).

Le théorème IV.2.9 peut être appliqué récursivement : afin de prouver l'égalité entre deux diagrammes avec n entrées, m sorties et des constantes dans $\frac{\pi}{4}\mathbb{Z}$, on peut considérer les 2^{n+m} façons de fixer ces entrées/sorties dans une base. L'existence d'une preuve entre deux diagrammes avec des constantes dans $\frac{\pi}{4}\mathbb{Z}$ se réduit alors à l'existence de preuves sur des diagrammes scalaires (diagrammes sans entrée et sans sortie).

Cas 2 – Considérer un ensemble fini d'angles

Nous pouvons également considérer un nombre fini d'angles. Nous montrons ici qu'il suffit de prouver une équation $D_1(\alpha^{(i)}) = D_2(\alpha^{(i)})$ pour un ensemble fini d'angles $\alpha^{(i)}$ pour en déduire que $ZX \vdash D_1(\alpha) = D_2(\alpha)$ avec un angle alpha arbitraire. Le choix des angles est relativement libre, en revanche le nombre d'angles à considérer dépend des diagrammes, en particulier de la multiplicité d'un angle dans une équation. La multiplicité d'un angle est intuitivement le maximum d'occurrences d'une variable dans chaque membre de l'équation (si α apparait 4 fois à gauche de l'égalité et 3 fois à droite, sa multiplicité sera de 4). Dans le cas où une variable α et son opposé $-\alpha$ apparaissent dans une équation alors on compte indépendamment le nombre d'occurrence de α et $-\alpha$ et on les additionne. Formellement :

Définition IV.2.10. *Pour toute paire $D_1(\alpha), D_2(\alpha) : n \to m$ de ZX-diagrammes linéaires en α, la multiplicité de α dans l'équation $D_1(\alpha) = D_2(\alpha)$ est :*

$$\mu_\alpha = \max_{i\in\{1,2\}} \left(\mu_\alpha^+(D_i(\alpha))\right) + \max_{i\in\{1,2\}} \left(\mu_\alpha^-(D_i(\alpha))\right)$$

où $\mu_\alpha^+(D)$ (resp. $\mu_\alpha^-(D)$) est le nombre d'occurences de α (resp. -α) dans D, inductivement défini :

$$\mu_\alpha^+(R_Z^{(n,m)}(\ell\alpha + c)) = \mu_\alpha^+(R_X^{(n,m)}(\ell\alpha + c)) = \begin{cases} \ell & si\ \ell > 0 \\ 0 & sinon \end{cases}$$

$$\mu_\alpha^-(R_Z^{(n,m)}(\ell\alpha + c)) = \mu_\alpha^-(R_X^{(n,m)}(\ell\alpha + c)) = \begin{cases} -\ell & si\ \ell < 0 \\ 0 & sinon \end{cases}$$

$\forall \diamond \in \{+, -\}$, $\mu_\alpha^\diamond(D \otimes D') = \mu_\alpha^\diamond(D \circ D') = \mu_\alpha^\diamond(D) + \mu_\alpha^\diamond(D')$

$\mu_\alpha^\diamond(H) = \mu_\alpha^\diamond(e) = \mu_\alpha^\diamond(\mathbb{I}) = \mu_\alpha^\diamond(\sigma) = \mu_\alpha^\diamond(\epsilon) = \mu_\alpha^\diamond(\eta) = 0$

Théorème IV.2.11. *Pour toute paire $D_1(\vec{\alpha}), D_2(\vec{\alpha}) : n \to m$ de ZX-diagrammes linéaire en $\vec{\alpha} = \alpha_1, \ldots, \alpha_k$ avec constante dans $\frac{\pi}{4}\mathbb{Z}$, si*

$$\forall \vec{\alpha} \in T_1 \times \ldots \times T_k, \mathrm{ZX} \vdash D_1(\vec{\alpha}) = D_2(\vec{\alpha})$$

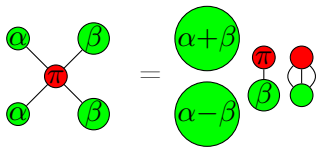
alors

$$\forall \vec{\alpha} \in \mathbb{R}^k, \mathrm{ZX}_T \vdash D_1(\vec{\alpha}) = D_2(\vec{\alpha})$$

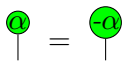
avec T_i un ensemble de $\mu_i + 1$ angles distincts dans $\mathbb{R}/2\pi\mathbb{Z}$ où μ_i est la multiplicité de α_i dans $D_1(\vec{\alpha}) = D_2(\vec{\alpha})$.

Par exemple dans l'équation suivante la multiplicité de α est $\mu_\alpha = 2$, donc il suffit de prouver cette équation pour 3 valeurs de α, par exemple $0, \pi$ et $\frac{\pi}{2}$ pour

qu'elle soit vraie pour tout α.



Remarque IV.2.12. *Le nombre d'occurrences d'une variable ne doit pas être confondu avec sa multiplicité. Considérons par exemple l'équation suivante :*



Cette équation est évidemment fausse en général, mais pas pour 0 *et* π*. Si nous essayons d'appliquer le théorème IV.2.11 avec le nombre d'occurrences (qui semble être* 1*), alors nous pourrions nous retrouver avec la mauvaise conclusion. La multiplicité (ici* $\mu_\alpha = 2$*) empêche cela.*

Cas 3 – Substitution de diagramme

Une dernière application pratique permettant de démontrer des équations du ZX-calcul avec des diagrammes linéaires est de faire de la substitution de diagrammes. Intuitivement si une équation contient un sous-diagramme commun aux deux membres de l'équation alors on peut tenter de prouver l'équation en remplaçant ce sous-diagramme par un simple nœud vert ou rouge avec un angle arbitraire.

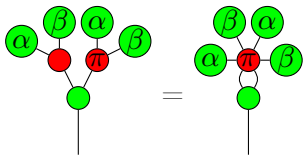
Théorème IV.2.13. *Pour toute paire* $D_1(\vec{\alpha}), D_2(\vec{\alpha}) : r \to n$ *de ZX-diagrammes, et pour tout diagramme* $D(\vec{\alpha}) : 0 \to 1$ *tels que* $D_1(\vec{\alpha})$*,* $D_2(\vec{\alpha})$*, et* $D(\vec{\alpha})$ *sont linéaires en* $\vec{\alpha}$ *avec constante dans* $\frac{\pi}{4}\mathbb{Z}$*,*

$$\forall \alpha_0 \in \mathbb{R}, \forall \vec{\alpha} \in \mathbb{R}^k, \quad \mathrm{ZX}_T \vdash \boxed{\begin{matrix}\alpha_0 & \alpha_0 \\ \cdots & \\ D_1(\vec{\alpha}) \\ \cdots\end{matrix}} = \boxed{\begin{matrix}\alpha_0 & \alpha_0 \\ \cdots & \\ D_2(\vec{\alpha}) \\ \cdots\end{matrix}}$$

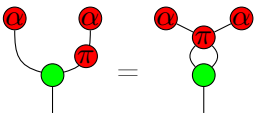
$$\Rightarrow \quad \forall \vec{\alpha} \in \mathbb{R}^k, \mathrm{ZX}_T \vdash \boxed{\begin{matrix}D(\vec{\alpha}) & \cdots & D(\vec{\alpha}) \\ D_1(\vec{\alpha}) \\ \cdots\end{matrix}} = \boxed{\begin{matrix}D(\vec{\alpha}) & \cdots & D(\vec{\alpha}) \\ D_2(\vec{\alpha}) \\ \cdots\end{matrix}}$$

Par exemple, on peut démontrer la généralisation suivante de la supplémentarité :

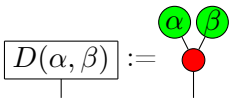
$$\forall \alpha, \beta \in \mathbb{R}^2, \quad \mathrm{ZX}_T \vdash$$



En utilisant (SUP) (en inversant les couleurs) et (S1) on peut prouver facilement :

$\forall \alpha \in \mathbb{R}, \quad \mathrm{ZX}_T \vdash$  $=$

En appliquant le Théoreme IV.2.13 avec



qui est clairement symétrique, et en utilisant (S1), on en déduit la généralisation de la supplémentarité.

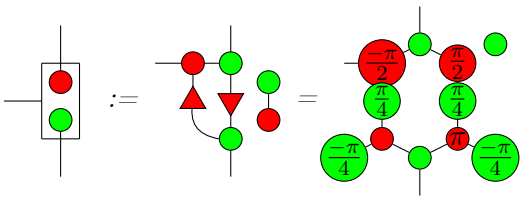
IV.2.3 Formes normales

Dans cette section nous introduisons une notion de forme normale pour les diagrammes du ZX-calcul. L'utilisation de formes normales permet notamment de prouver la complétude du langage (ou d'un fragment du langage) directement sans utiliser une traduction vers un autre langage. Nous utilisons ici les formes normales pour montrer la complétude de plusieurs fragments du langage, notamment celui des angles dyadiques et le langage en général.

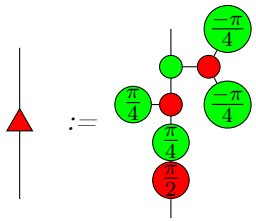
Nous formalisons ici la notion générale de fragment du ZX-calcul : étant donné un sous groupe additif G de $\mathbb{R}/2\pi\mathbb{Z}$, ZX^G désigne l'ensemble des diagrammes dont tous les angles sont dans G. On note $\mathcal{G}$ l'ensemble des sous groupes additifs de $\mathbb{R}/2\pi\mathbb{Z}$ qui contiennent $\frac{\pi}{4}$. L'interprétation d'un ZX^G-diagramme est une matrice à coefficients dans l'anneau $\mathcal{R}_G := \mathbb{Z}\left[\frac{1}{\sqrt{2}}, e^{iG}\right]$.

Les formes normales que nous introduisons reposent largement sur le concept de diagramme contrôlé. Pour définir les diagrammes controlés nous utilisons un gadget particulier agissant comme un transistor :

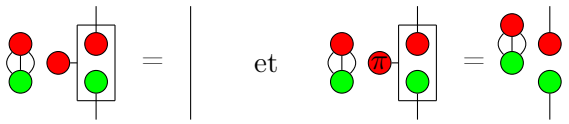
Définition IV.2.14. *Nous définissons le* transistor *comme le diagramme à trois branches :*



où nous utilisons la notation 'triangle' suivante :



On peut vérifier que :



Il peut être vu comme un commutateur contrôlé : si $|0\rangle$ est branché à gauche, le fil droit est intact, mais si $|1\rangle$ est branché à gauche, le fil droit est "ouvert" par l'opération.

Les états contrôlés forment une famille particulière de ZX-diagrammes avec une seule entrée et n sorties, leur interprétation associe à $|0\rangle$ la superposition uniforme $\sum_{x\in\{0,1\}^n} |x\rangle$. Intuitivement, un état contrôlé $D : 1 \to n$ est juste un encodage pour l'état $[\![D]\!]\,|1\rangle$.

Définition IV.2.15 (États contrôlés)**.** *Un ZX-diagramme $D : 1 \to n$ est un* état contrôlé *si* $[\![D]\!]\,|0\rangle = \sum_{x\in\{0,1\}^n} |x\rangle$.

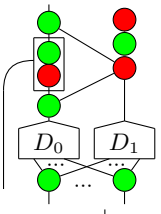
Un état contrôlé sans sortie est appelé scalaire contrôlé :

Définition IV.2.16 (Scalaires contrôlés)**.** *Un* ZX*-diagramme $D : 1 \to 0$ est un* scalaire contrôlé *si* $[\![D]\!]\,|0\rangle = 1$.

Dans la famille des diagrammes d'états contrôlés, nous définissons ceux qui sont en forme normale. Notre définition de forme normale est générique en ce sens qu'elle est définie par rapport à un ensemble donné de scalaires contrôlés. Intuitivement, le choix de ces scalaires contrôlés dépend du fragment considéré du langage, comme détaillé dans les sections suivantes.

Définition IV.2.17 (Forme Normale Contrôlée)**.** *Étant donné un ensemble S de scalaires contrôlés, les diagrammes en S-forme normale contrôlée (S-*CNF*) sont définis de manière inductive comme suit :*

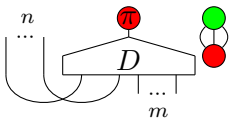
— $\forall D \in S$, *D est en S-*CNF *;*

— $\forall D_0, D_1 : 1 \to n$ *sont* S-CNF,  $: 1 \to 1+n$ *est en* S-CNF.

Un diagramme D *en* S-CNF *est représenté*  .

On peut vérifier que les diagrammes sous forme normale contrôlée sont en fait des états contrôlés : si $D : 1 \to n$ est en S-CNF, alors $[\![D]\!] |0\rangle = \sum_{x \in \{0,1\}^n} |x\rangle$.

Nous sommes maintenant prêts à donner une définition des diagrammes sous forme normale, basée sur les diagrammes sous forme normale contrôlée :

Définition IV.2.18 (Forme Normale)**.** *Étant donné un ensemble* S *de scalaires contrôlés, pour tout* $n, m \in \mathbb{N}$*, et tout* $D : 1 \to n+m$ *en* S-CNF, 

est en forme normale *par rapport à* S *(*S-NF*).*

Universalité

Bien que l'application principale de la notion de forme normale est de prouver des résultats de complétude, notre première application est de prouver l'universalité de ZX^G pour tout $G \in \mathcal{G}$.

Théorème IV.2.19. *Pour tout* $G \in \mathcal{G}$*,* ZX^G *est universel :*

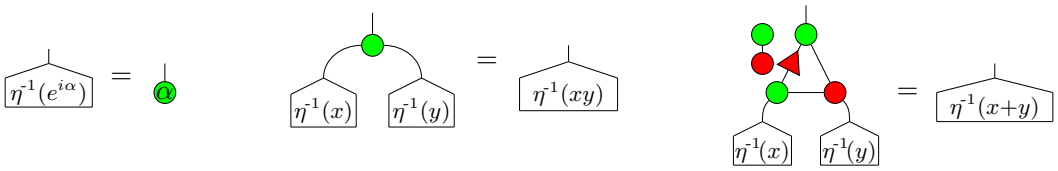
$$\forall n, m \in \mathbb{N}, \forall M \in \mathcal{R}_G^{2^n \times 2^m}, \exists D \in ZX^G, [\![D]\!] = M$$

Une condition suffisante de complétude

Les *états contrôlés* donnent une structure interne générique pour un diagramme en forme normale, en séparant les coefficients du processus – relatifs au fragment considéré – de la façon dont ils sont combinés – ce qui est fait dans le fragment $\frac{\pi}{4}$. Par conséquent, toutes les opérations correctes sur la *structure* des formes normales devraient être réalisables en utilisant l'ensemble de règles ZX_T-calcul (figure IV.2). La complétude des plus grands fragments est alors réduite à la capacité à appliquer des opérations élémentaires aux coefficients :

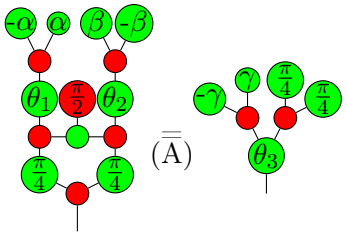
Théorème IV.2.20 (Condition suffisante de complétude)**.** *Étant donné* $G \in \mathcal{G}$*,* ZX^G *est complet si* $\exists S \subseteq \mathrm{ZX}^G$ *un ensemble de scalaires contrôlés tels que* $\eta : S \to$

$\mathcal{R}_G = D \mapsto [\![D]\!]\,|1\rangle$ *est bijective et que les équations suivantes sont satisfaites :* $\forall \alpha \in G, \forall x, y \in \mathcal{R}_G$,



IV.2.4 Formes normales avec des angles arbitraires

Dans le cas où les angles sont arbitraires, il suffit d'ajouter l'axiome suivant pour rendre le langage complet



$$e^{i\theta_1}\cos(\alpha) + e^{i\theta_2}\cos(\beta) = 2e^{i\theta_3}\cos(\gamma)$$

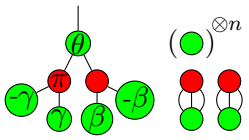
Dans la suite, ZX_T augmenté de l'axiome (A) sera noté ZX_A.

Afin de prouver la complétude de ZX_A en utilisant les forme normale générique, nous définissions tout d'abord les scalaires controlés, qui sont spécifiques au fragment général $\mathrm{ZX}^{\mathbb{R}/2\pi\mathbb{Z}}$:

Définition IV.2.21. *Soit* $\Lambda_{\mathbb{R}} : \mathbb{C} \to \mathrm{ZX}[1,0]$ *– où* $\mathrm{ZX}[1,0]$ *désigne l'ensemble des ZX-diagramme de type* $1 \to 0$ *– défini telle que :*

— $\Lambda_{\mathbb{R}}(0) =$ 

— $\forall \rho > 0, \forall \theta \in [0, 2\pi)$,

$$\Lambda_{\mathbb{R}}(\rho e^{i\theta}) :=$$ 

$$\left(\begin{array}{l} n := \max\left(0, \lceil \log_2(\rho) \rceil\right) \\ \beta := \arccos(\frac{\rho}{2^n}) \\ \gamma := \arccos(\frac{1}{2^n}) \end{array}\right)$$

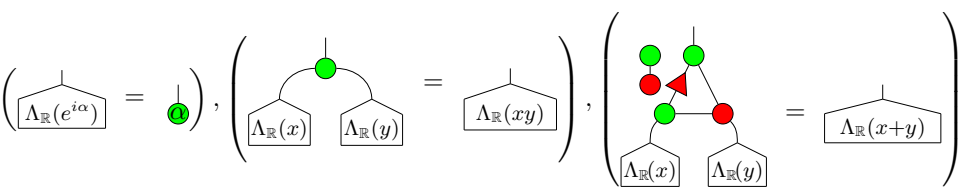
et $S_{\mathbb{R}} := \{\Lambda_{\mathbb{R}}(x) \mid x \in \mathbb{C}\}$.

On peut vérifier qu'il s'agit bien de scalaires contrôlés :

Lemme IV.2.22. *Pour tout* $x \in \mathbb{C}$, $\Lambda_{\mathbb{R}}(x)$ *est un scalaire contrôlé et* $[\![\Lambda_{\mathbb{R}}(x)]\!]\,|1\rangle = x$.

Afin d'appliquer le théorème IV.2.20, il faut vérifier que les 3 équations sur les scalaires contrôlés sont satisfaites :

Lemme IV.2.23. *La fonction* $\eta_{\mathbb{R}} : S_{\mathbb{R}} \to \mathcal{R}_G = D \mapsto [\![D]\!]\,|1\rangle$ *est bijective et* $\Lambda_{\mathbb{R}} = \eta_{\mathbb{R}}^{-1}$. *De plus :*

$\mathrm{ZX}^{\mathrm{A}} \vdash$ 

Théorème IV.2.24. *Le ZX-calcul général (sans restriction sur les angles) est complet avec l'axiome* ZX_{A}.

Cette preuve de complétude de ZX_{A} est une application intéressante des formes normales génériques, mais il est important de noter que la complétude de ZX_A a été originellement démontrée sans utiliser les formes normales : dans [61] nous avons montré la complétude de ZX_A en utilisant une traduction directe avec une extension du $\mathrm{ZW}_{\mathbb{C}}$-calcul qui a été montrée complète par [51]. Cette preuve est basée sur l'utilisation de diagrammes linéaires (voir section IV.2.2).

La complétude du ZX_A améliore un résultat [52] de Ng et Wang qui ont démontré la complétude d'une variante du ZX-calcul qui non seulement possède plus d'axiomes (environ deux fois plus) mais aussi deux générateurs supplémentaires, ce qui change de façon assez importante la nature du langage. Cette preuve s'appuie également sur une traduction entre ZX-calcul et $\mathrm{ZW}_{\mathbb{C}}$-calcul.

IV.2.5 Complétude pour angles rationnels

Dans cette section nous considérons des fragments pour lesquels l'utilisation des formes normales génériques a permis d'établir de nouveaux résultats de complétude.

En utilisant les formes normales générique on peut montrer qu'un seul axiome additionnel, d'ordre supérieur, permet de rendre $\mathrm{ZX}^{\frac{\pi}{4n}}$ complet, avec $n \in \mathbb{N}^*$ où les angles sont des multiples de $\frac{\pi}{4n}$.

Théorème IV.2.25. *Le fragment* $\frac{\pi}{4n}$ *du ZX-calculus avec les équations de la figure IV.2 et la méta-règle suivante de simplification est complet.*

$$\forall \alpha \neq \pi \bmod 2\pi, \quad \mathrm{ZX} \vdash D_1 \otimes \boxed{\alpha} = D_2 \otimes \boxed{\alpha} \underset{\text{(cancel)}}{\Longrightarrow} \mathrm{ZX} \vdash D_1 = D_2$$

On note $\mathrm{ZX}_{\mathrm{cancel}}$ pour ZX_T augmenté du méta-axiome (cancel). Le théorème IV.2.25 permet plus généralement de démontrer la complétude de tout fragment $\mathrm{ZX}_{\mathrm{cancel}}$ avec $G \subset \pi\mathbb{Q}$ sous groupe d'angles rationnels incluant $\frac{\pi}{4}$.

De plus il s'avère que l'axiome de simplification est démontrable pour les angles dyadiques, i.e. des angles multiples de $\frac{\pi}{2^n}$, on en déduit :

Théorème IV.2.26. *Le fragment $\frac{\pi}{2^{n+1}}$ du ZX-calculus avec les équations de la figure IV.2 est complet.*

En résumé, nous avons obtenu les résultats de complétudes suivants :

Fragments	Axiomatisation Complète
$G \subseteq \mathbb{D}\pi$	ZX^G
$G \subseteq \mathbb{Q}\pi$	$\mathrm{ZX}^G_{\mathrm{cancel}}$
Général	ZX^{A}

Récemment, Emmenuel Jeandel a montré que dans le cas du fragment rationnel la méta-règle de simplification (cancel) peut être remplacée par les règles de supplémentarité cyclotomique ($Supp_p$) avec p premier [58].

Chapitre V

Les différents ZX-calculs

Nous reprenons dans ce chapitre les différentes variantes du ZX-calcul rencontrées dans ce mémoire.

ZX_0-calcul

Le ZX_0-calcul est le calcul originel – à des scalaires de renormalisation près – introduit par Coecke et Duncan [28].

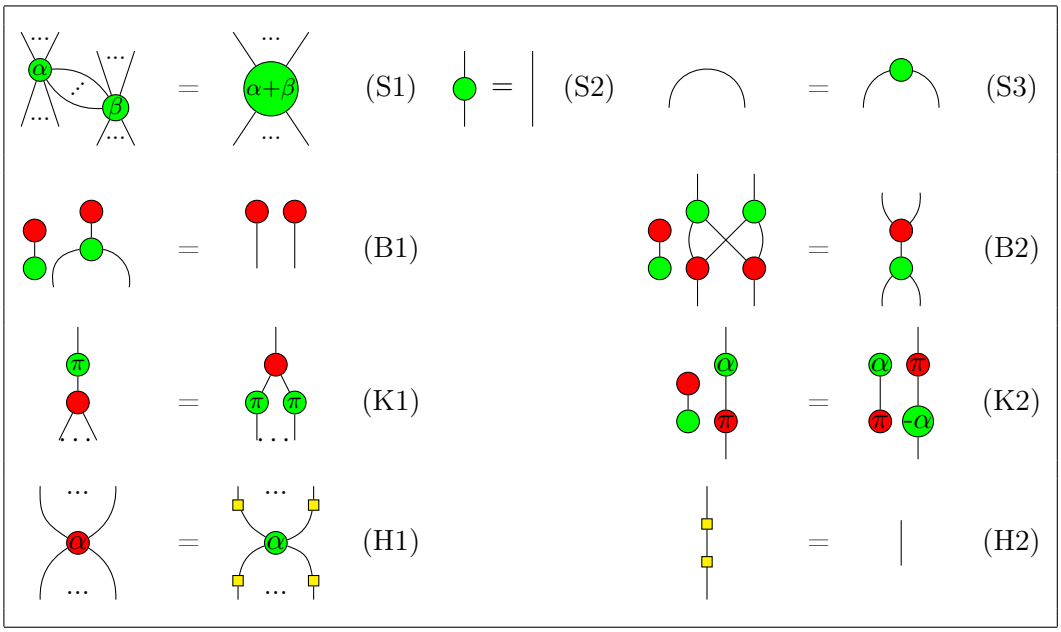


Table V.1 – ZX_0-calcul

$\mathbf{ZX}_H$-calcul

Le ZX_H-calcul correspond au ZX_0-calcul augmenté de la décomposition d'Euler de H.

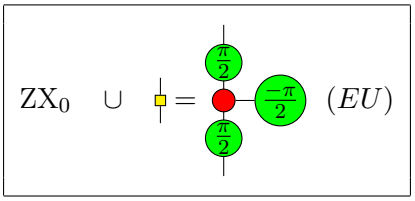


TABLE V.2 – ZX_H-calcul

$\mathbf{ZX}_s$-calcul

Le ZX_s-calcul correspond au ZX_H augmenté de deux axiomes pour les scalaires

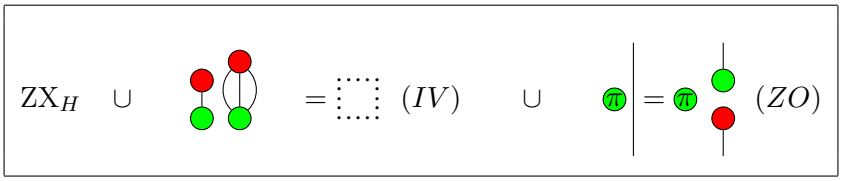


TABLE V.3 – ZX_s-calcul

Le ZX_s-calcul est complet pour le fragment stabilisable de la mécanique quantique (Clifford) [7, 10].

$\mathbf{ZX}_E$-calcul

Le ZX_E-calcul correspond au ZX_s augmenté de l'axiome (E) sur les scalaires, spécifique au fragment $\frac{\pi}{4}$.

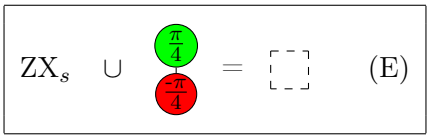


TABLE V.4 – ZX_E-calcul

$\mathbf{ZX_{supp}}$-calcul

Le $\mathrm{ZX}_{\mathrm{supp}}$-calcul correspond au ZX_E augmenté de la supplémentarité (SUP). La règle sur les scalaires (IV) est démontrable en utilisant les autres axiomes du $\mathrm{ZX}_{\mathrm{supp}}$-calcul, on en déduit l'axiomatisation suivante :

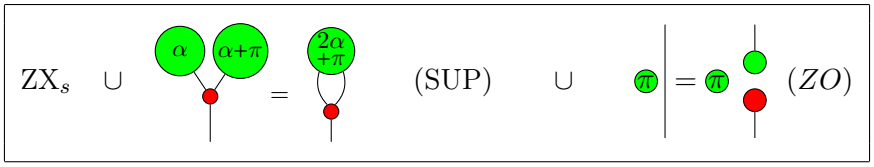


TABLE V.5 – $\mathrm{ZX}_{\mathrm{supp}}$-calcul

$\mathbf{ZX_{cyclo}}$-calcul

Le $\mathrm{ZX}_{\mathrm{cyclo}}$-calcul correspond au $\mathrm{ZX}_{\mathrm{supp}}$ augmenté de la supplémentarité cyclotomique (SUP_n), pour tout n premier.

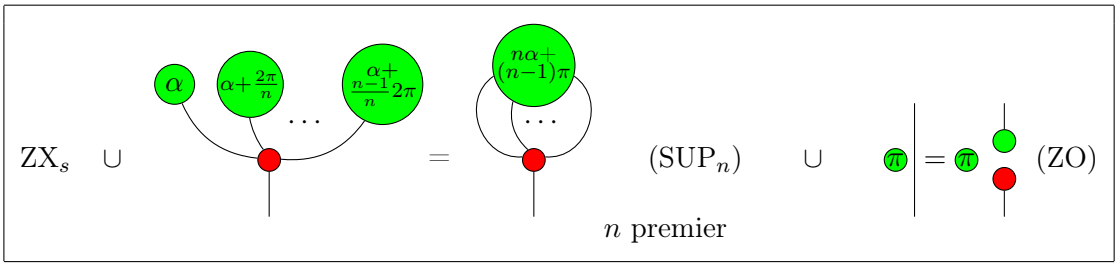


TABLE V.6 – $\mathrm{ZX}_{\mathrm{cyclo}}$-calcul

$\mathbf{ZX}_T$-calcul

Le ZX_T-calcul correspond au $\mathrm{ZX}_{\mathrm{supp}}$ augmenté de deux axiomes (C) et (BW). Le fragment $\frac{\pi}{4}$ du ZX_T-calcul est complet pour Clifford+T.

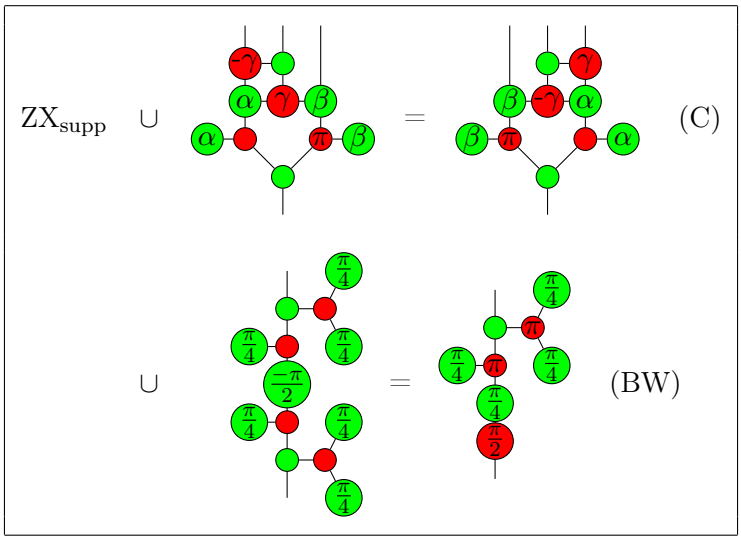


TABLE V.7 – ZX$_T$-calcul

ZX$_A$-calcul

Le ZX$_A$-calcul correspond au ZX$_T$ augmenté de l'axiome (A) non linéaire. Le ZX$_A$-calcul est complet pour la mécanique quantique pure à base de qubits (sans restriction sur les angles).

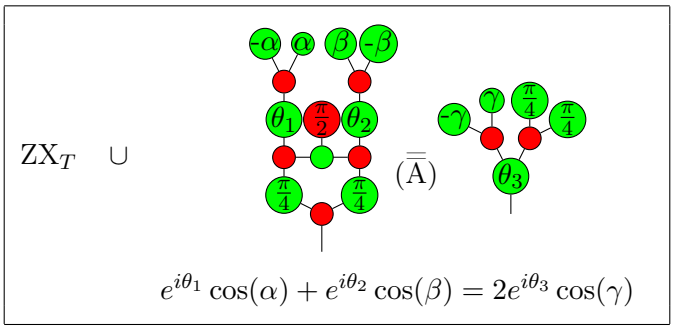


TABLE V.8 – ZX$_A$-calcul

$\mathbf{ZX_{cancel}}$-calcul

Le $\mathrm{ZX}_{\mathrm{cancel}}$-calcul correspond au ZX_T augmenté de la méta-règle (cancel) qui permet de simplifier un scalaire non nul. Le $\mathrm{ZX}_{\mathrm{cancel}}$-calcul est complet pour tout fragment rationnel.

$\mathrm{ZX}_T \quad \cup \quad \forall \alpha \neq \pi \bmod 2\pi, \quad \mathrm{ZX} \vdash D_1 \otimes \boxed{\alpha} = D_2 \otimes \boxed{\alpha} \underset{\text{(cancel)}}{\Longrightarrow} \mathrm{ZX} \vdash D_1 = D_2$ (cancel)

TABLE V.9 – $\mathrm{ZX}_{\mathrm{cancel}}$-calcul

Chapitre VI

Perspectives

Je termine ce manuscrit par mon projet de recherche à moyen terme :

Utiliser l'Ordinateur Quantique

Mon projet de recherche s'inscrit dans la continuité de mes travaux actuels de recherche autour des approches graphiques en informatique quantique. Il vise à faciliter les interactions entre l'approche théorique du calcul quantique et les efforts technologiques déployés pour mettre en œuvre l'ordinateur quantique.

Contexte.
L'informatique quantique est un sujet de recherche en plein essor. Un traitement quantique de l'information permet en théorie de résoudre certains problèmes informatiques hors de portée des ordinateurs classiques. Les programmes britannique (NQIT [1]), néerlandais (QuTech [2]), et surtout européen (Flagship sur les Technologies Quantiques [3]), ainsi que la fabrication (voire la commercialisation) de machines quantiques de plusieurs dizaines de qubits par Google, IBM ou encore par des start-up comme Rigetti [4] ou D-Wave [5], démontrent que l'informatique quantique est en train d'entrer dans une nouvelle ère.

Problématique.
L'ordinateur quantique en est encore à ses balbutiements et plusieurs technologies sont concurrentes (ion-trap, supra-conducteur, solid states, optique ...) pour la mise

1. Networked Quantum Information Technologies, http ://nqit.ox.ac.uk
2. Quantum Technology, http ://qutech.nl
3. https ://ec.europa.eu/digital-single-market/en/quantum-technologies
4. http ://rigetti.com
5. http ://www.dwavesys.com

en œuvre de l'ordinateur quantique. Nous visons à combler l'écart entre les algorithmes quantiques théoriques et ces différentes technologies. De plus, l'émergence de prototypes de machines quantiques est très prometteuse, mais ouvre aussi des nouvelles problématiques concrètes comme la **programmation** et la **vérification quantique** de ces machines. Le développement d'outils de méthodes formelles permettant le développement et, à terme, l'**utilisation** de machines quantiques est donc essentiel.

Approche.
Pour développer des outils efficaces pour l'ordinateur quantique, il est primordial de comprendre les spécificités du traitement quantique de l'information. Nous avons vu dans ce manuscrit que dans de nombreux domaines de l'informatique quantique une approche graphique s'est imposée : circuits quantiques, états graphes, ZX-calcul sont donc des exemples de développements réussis de langages graphiques dans le traitement quantique de l'information. Il y a des raisons intrinsèques à ce succès : le picturalisme capture des propriétés quantiques fondamentales comme l'intrication, la contextualité, la causalité et comment elles interagissent dans l'espace-temps.

Objectifs.
Mon objectif est de mettre à contribution mon expertise dans ces différents domaines, pour développer des outils permettant l'analyse, la vérification et plus généralement l'utilisation de l'ordinateur quantique. Une chaîne de compilation quantique permet de faire le lien entre les algorithmes quantiques, décrits dans des langages de haut niveau, et les technologies quantiques vers lesquelles ces algorithmes vont être compilés puis exécutés. Les projets ANR SoftQPro – dont je suis le responsable – et BPI/GIA Quantex qui ont débuté fin 2017, début 2018 visent à développer de telles chaînes de compilation.

Dans ces chaînes de compilation, le ZX-calcul joue le rôle de représentation intermédiaire entre langage de haut niveau, utilisé par le développeur pour décrire des algorithmes quantiques, et les différents langages de bas niveaux, liés aux différentes architectures, modèles de calcul ou technologies quantiques considérés. Plus expressifs que le modèle des circuits quantiques, les ZX-diagrammes peuvent représenter différents modèles de calcul (calcul par circuits, ou calcul par mesures par exemple) et s'adapter aux différentes contraintes des technologies quantiques. Équipé d'une puissante théorie équationnelle, que nous avons montré complète, le ZX-calcul peut être utilisé pour optimiser ou plus généralement transformer du code.

Je liste ci-dessous des problématiques concrètes sur lesquelles je souhaite travailler.

Optimisation et Extraction de ZX-diagrammes. La complétude du ZX-calcul ouvre des perspectives immenses d'utilisation de ZX-calcul pour l'optimisation d'algorithmes quantiques. En effet, comme aucune théorie équationnelle complète n'est connue pour les circuits quantiques, il est naturel d'utiliser les ZX-diagrammes. Il reste cependant plusieurs défis :

— Bien que le langage soit complet, optimiser un diagramme nécessite une stratégie qui dépend de l'objectif à atteindre : minimiser le nombre de portes, la profondeur, ou le nombre d'opérations non Clifford (plus difficiles à implémenter dans plusieurs technologies).

— L'extraction de diagrammes : une fois le diagramme optimisé, il faut être capable d'en extraire une séquence d'instructions implémentables.

Nous considérons actuellement avec Ross Duncan et Aleks Kissinger le cas concret de l'optimisation de circuits : à partir d'un circuit quantique, nous le transformons en ZX-diagramme, et appliquons des règles de simplification qui permettent de réduire le nombre de nœuds. Le challenge est alors d'extraire de ce diagramme optimisé un circuit quantique. Nous utilisons dans ce cas des techniques de *gflow* – que j'ai contribué à développer dans le cadre du calcul par mesure – comme d'une stratégie pour l'extraction de circuit.

Je souhaite poursuivre cette collaboration en cours sur l'optimisation de circuits et aussi m'attaquer au cas plus général des ZX-diagrammes qui ne sont pas nécessairement obtenus à partir de circuit quantique.

Calcul quantique robuste. Rendre le calcul quantique tolérant aux fautes est sans doute le principal défi de la construction de l'ordinateur quantique. Je souhaite travailler sur deux aspects importants de l'utilisation des codes correcteurs d'erreur :

— L'objectif est de développer le ZX-calcul pour permettre de représenter de façon plus compacte certains diagrammes très réguliers, en autorisant par exemple certains fils à représenter plusieurs qubits. Avec Titouan Carette, actuellement en première année de thèse nous travaillons au développement d'un ZX-calcul qui passe plus facilement à l'échelle. Un tel ZX-calcul permet de représenter de façon compacte des codes correcteurs et d'analyser la propagation des erreurs par exemple.

— Niel de Beaudrap et Dominic Horsman [37] ont montré que le ZX-calcul est un langage adapté à la représentation des codes surfaciques et à l'utilisation de techniques de "Lattice Surgery" qui y sont associés. L'objectif ici est de développer des techniques permettant de transformer un ZX-diagramme quelconque en un diagramme sémantiquement équivalent, mais adapté aux codes surfaciques, pour permettre une implémentation tolérante aux fautes.

Contraintes issues de la physique. Mon objectif est également de considérer de façon plus précise des contraintes technologiques issues de la physique, afin de tenir compte de ces contraintes dans la représentation et la transformation de diagrammes.

— Par exemple, en optique quantique, beaucoup de physiciens préfèrent travailler avec des variables continues (système de dimension infinie) plutôt que des qubits. L'objectif est de développer des outils comme les états graphes ou le ZX-calcul pour représenter, manipuler et analyser des systèmes à base de variables continues. C'est le sujet de la thèse de Robert Booth qui a débuté en novembre 2018 que je co-encadre avec Damian Markham.

— Plus généralement, il est important de tenir compte des contraintes issues des technologies quantiques. Avec des collègues grenoblois, dans le cadre d'un consortium formé d'informaticiens et de physiciens, nous avons déposé un proposition de projet ANR visant à développer des outils de méthodes formels, en étant au plus près des spécificités technologiques, en l'occurrence celles des technologies à base de silicium développées au CEA Grenoble.

Le contrôle quantique. En informatique quantique, le paradigme "données quantiques, contrôle classique" est souvent retenu, cela signifie que la mémoire de l'ordinateur est quantique en revanche le contrôle, par exemple l'ordre des opérations, est purement classique. Le modèle des circuits quantiques et la plupart des langages de programmation quantique suivent ce paradigme. Le paradigme a pourtant des limites. D'un point de vue fondamental, plusieurs travaux portent sur le contrôle quantique, notamment dans l'ordre d'exécution des opérations [27, 42, 44, 1]. D'un point de vue plus pragmatique, même dans les langages de programmation comme Quipper [49] ou dans le modèle des circuits quantiques il y a une certaine forme de contrôle quantique, en autorisant toute opération unitaire U à être contrôlée : pour toute transformation unitaire U, contrôle-U (notée ΛU) est la transformation unitaire $\Lambda U : |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$. Ainsi, si le qubit de contrôle est dans l'état $|1\rangle$ on applique U sur les autres qubits, si il est dans l'état $|0\rangle$ on applique l'identité. Il s'agit d'un contrôle quantique : si le qubit de contrôle est en superposition de $|0\rangle$ et $|1\rangle$ on applique U et l'identité en superposition.

La question est ici de représenter un tel contrôle quantique en ZX-calcul et comprendre s'il peut être étendu à des opérations non-unitaires, ce qui semble être réalisable expérimentalement [27].

Bibliography

[1] A. A. Abbott, J. Wechs, D. Horsman, M. Mhalla, and C. Branciard. Communication through coherent control of quantum channels. *arXiv preprint arXiv:1810.09826*, 2018.

[2] S. Abramsky and B. Coecke. A categorical semantics of quantum protocols. In *LICS*, pages 415–425, 2004.

[3] S. Abramsky and B. Coecke. A categorical semantics of quantum protocols. In *Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science (LICS)*. IEEE Computer Society, 2004. Also arXiv:quant-ph/0402130.

[4] M. Amy, J. Chen, and N. J. Ross. A finite presentation of CNOT-dihedral operators. In B. Coecke and A. Kissinger, editors, Proceedings 14th International Conference on *Quantum Physics and Logic,* Nijmegen, The Netherlands, 3-7 July 2017, volume 266 of *Electronic Proceedings in Theoretical Computer Science*, pages 84–97. Open Publishing Association, 2018.

[5] P. Arrighi and S. Perdrix. Modèle de calcul quantique. *Informatique Mathématique, une photographie en 2016, CNRS Alpha*, 2016.

[6] A. Aspect, J. Dalibard, and G. Roger. Experimental test of Bell's inequalities using time-varying analyzers. *Phys. Rev. Lett.*, 49(25):1804–1807, 1982.

[7] M. Backens. The ZX-calculus is complete for stabilizer quantum mechanics. In *Quantum Physics and Logic (QPL 2012)*, 2012.

[8] M. Backens. The ZX-calculus is complete for the single-qubit Clifford+T group. *Electronic Proceedings in Theoretical Computer Science*, 172:293–303, dec 2014.

[9] M. Backens and A. Kissinger. ZH: A complete graphical calculus for quantum computations involving classical non-linearity, 2018.

[10] M. Backens, S. Perdrix, and Q. Wang. A simplified stabilizer zx-calculus. *arXiv preprint arXiv:1602.04744*, 2016.

[11] J. C. Baez and J. Erbele. Categories in control. *Theory and Applications of Categories*, 30(24):836–881, 2015.

[12] J. Bell. On the Einstein Podolsky Rosen paradox. *Physics*, 1:195, 1964.

[13] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE international Conference on Computers, Systems and Signal Processing, Bangalore, India*, page 175, New York, 1984. IEEE Press.

[14] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, 1993.

[15] C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on Einstein -Podolsky- Rosen states. *Phys. Rev. Lett.*, 69:2881–2884, 1992.

[16] X. Bian and Q. Wang. Graphical calculus for qutrit systems. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 98(1):391–399, 2015.

[17] F. Bonchi, P. Sobociński, and F. Zanasi. Interacting Hopf algebras. *Journal of Pure and Applied Algebra*, 221(1):144–184, 2017.

[18] A. Bouchet. Connectivity of isotropic systems. In N. Y. A. of Sciences, editor, *Proceedings of the third international conference on Combinatorial mathematics*, pages 81–93, 1989.

[19] A. Broadbent, P.-R. Chouha, and A. Tapp. The GHZ State in Secret Sharing and Entanglement Simulation. In *International Conference on Quantum, Nano, and Micro Technologies*, 2009.

[20] A. Broadbent, J. Fitzsimons, and E. Kashefi. Universal blind quantum computation. In *50th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2009*, 2009.

[21] A. Broadbent and E. Kashefi. Parallelizing quantum circuits. *Theoretical Computer Science*, 410(26):2489–2510, 2007.

[22] D. E. Browne, E. Kashefi, M. Mhalla, and S. Perdrix. Generalized flow and determinism in measurement-based quantum computation. *New Journal of Physics (NJP)*, 9(8), 2007.

[23] D. E. Browne, E. Kashefi, and S. Perdrix. Computational depth complexity of measurement-based quantum computation. In *Theory of Quantum Computation, Communication, and Cryptography (TQC'10)*, volume 6519, pages 35–46. LNCS, 2011.

[24] D. Cattanéo and S. Perdrix. Parameterized complexity of weak odd domination problems. In *Fundamentals of Computation Theory*, pages 107–120. Springer, 2013.

[25] D. Cattanéo and S. Perdrix. Minimum Degree up to Local Complementation: Bounds, Parameterized Complexity, and Exact Algorithms. In *26th International Symposium on Algorithms and Computation (ISAAC 2015)*, volume 9472 of *LNCS*, page 12, Nagoya, Japan, Dec. 2015.

[26] M. Cesati. The turing way to parameterized complexity. *Journal of Computer and System Sciences*, 67:654–685, 2003.

[27] G. Chiribella, G. M. D'Ariano, P. Perinotti, and B. Valiron. Quantum computations without definite causal structure. *Physical Review A*, 88(2):022318, 2013.

[28] B. Coecke and R. Duncan. Interacting quantum observables. In *ICALP (2)*, pages 298–310, 2008.

[29] B. Coecke and B. Edwards. Three qubit entanglement within graphical Z/X-calculus. *arXiv preprint arXiv:1103.2811*, 2011.

[30] B. Coecke and A. Kissinger. The compositional structure of multipartite quantum entanglement. In *Automata, Languages and Programming*, pages 297–308. Springer Berlin Heidelberg, 2010.

[31] B. Coecke and A. Kissinger. *Picturing Quantum Processes: A First Course in Quantum Theory and Diagrammatic Reasoning*. Cambridge University Press, 2017.

[32] B. Coecke, D. Pavlovic, and J. Vicary. A new description of orthogonal bases. *Mathematical Structures in Computer Science*, 23(3):555–567, 2013.

[33] B. Coecke and S. Perdrix. Environment and classical channels in categorical quantum mechanics. *Logical Methods in Computer Science*, Volume 8, Issue 4, Nov. 2012.

[34] V. Danos and E. Kashefi. Determinism in the one-way model. *Physical Review A*, 74(052310), 2006.

[35] V. Danos, E. Kashefi, and P. Panangaden. The measurement calculus. *J. ACM*, 54(2), 2007.

[36] V. Danos, E. Kashefi, P. Panangaden, and S. Perdrix. *Extended Measurement Calculus*. Cambridge University Press, 2010.

[37] N. de Beaudrap and D. Horsman. The ZX calculus is a language for surface code lattice surgery. *CoRR*, abs/1704.08670, 2017.

[38] R. Downey, M. Fellows, A. Vardy, and G. Whittle. The parameterized complexity of some fundabmental problems in coding theory. Technical Report 052, CDMTCS Research Report Series, 1997.

[39] R. Duncan and S. Perdrix. Graph states and the necessity of Euler decomposition. In *Conference on Computability in Europe*, pages 167–177. Springer, 2009.

[40] R. Duncan and S. Perdrix. Rewriting Measurement-Based Quantum Computations with Generalised Flow. In *International Colloquium on Automata, Languages and Programming (ICALP)*, pages 285–296, 2010.

[41] R. Duncan and S. Perdrix. Pivoting makes the ZX-calculus complete for real stabilizers. In *QPL 2013*, Electronic Proceedings in Theoretical Computer Science, pages 50–62, 2013.

[42] D. Ebler, S. Salek, and G. Chiribella. Enhanced communication with the assistance of indefinite causal order. *Physical review letters*, 120(12):120502, 2018.

[43] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of reality be considered complete? *Phys. Rev.*, 47(10):777–780, May 1935.

[44] S. Facchini and S. Perdrix. Quantum circuits for the unitary permutation problem. In *TAMC 2015*, volume 9076 of *Theory and Applications of Models of Computation*, pages 324–331, Singapore, Singapore, May 2015.

[45] P. Golovach, J. Kratochvil, and O. Suchy. Parameterized complexity of generalized domination problems. *Discrete Applied Mathematics*, 160:780–792, 2009.

[46] D. Gottesman. Theory of quantum secret sharing. *Phys. Rev. A*, 61:042311, Mar 2000.

[47] S. Gravier, J. Javelle, M. Mhalla, and S. Perdrix. On weak odd domination and graph-based quantum secret sharing. *CoRR*, abs/1112.2495, 2011.

[48] S. Gravier, J. Javelle, M. Mhalla, and S. Perdrix. Quantum secret sharing with graph states. In A. Kucera, T. A. Henzinger, J. Nesetril, T. Vojnar, and D. Antos, editors, *MEMICS*, volume 7721 of *Lecture Notes in Computer Science*, pages 15–31. Springer, 2012.

[49] A. S. Green, P. L. Lumsdaine, N. J. Ross, P. Selinger, and B. Valiron. Quipper: a scalable quantum programming language. In *ACM SIGPLAN Notices*, volume 48, pages 333–342. ACM, 2013.

[50] A. Hadzihasanovic. A diagrammatic axiomatisation for qubit entanglement. In *2015 30th Annual ACM/IEEE Symposium on Logic in Computer Science*, pages 573–584, July 2015.

[51] A. Hadzihasanovic. *The algebra of entanglement and the geometry of composition*. PhD thesis, University of Oxford, 2017.

[52] A. Hadzihasanovic, K. F. Ng, and Q. Wang. Two complete axiomatisations of pure-state qubit quantum computing. In *Proceedings of the 33rd Annual*

ACM/IEEE Symposium on Logic in Computer Science, LICS '18, pages 502–511, New York, NY, USA, 2018. ACM.

[53] M. Hein, J. Eisert, and H. J. Briegel. Multiparty entanglement in graph states. *Phys. Rev. A*, 69:062311, 2004.

[54] P. Høyer, M. Mhalla, and S. Perdrix. Resources required for preparing graph states. In *Proceedings of ISAAC06, LNCS*, volume 4288, pages 638–649, 2006.

[55] P. Høyer and R. Spalek. Quantum fan-out is powerful. *Theory of Computing*, 1(1):81–103, 2005.

[56] J. Javelle, M. Mhalla, and S. Perdrix. New protocols and lower bound for quantum secret sharing with graph states. In *Theory of Quantum Computation, Communication, and Cryptography (TQC'12)*, 09 2012.

[57] J. Javelle, M. Mhalla, and S. Perdrix. On the minimum degree up to local complementation: Bounds and complexity. In *Workshop on Graph-Theoretic Concepts in Computer Science (WG)*, volume abs/1204.4564, 2012.

[58] E. Jeandel. The rational fragment of the zx-calculus. *arXiv preprint arXiv:1810.05377*, 2018.

[59] E. Jeandel, S. Perdrix, and R. Vilmart. Y-calculus: A language for real matrices derived from the zx-calculus. *arXiv preprint arXiv:1702.00934*, 2017.

[60] E. Jeandel, S. Perdrix, and R. Vilmart. A complete axiomatisation of the ZX-calculus for Clifford+T quantum mechanics. In *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS '18, pages 559–568, New York, NY, USA, 2018. ACM.

[61] E. Jeandel, S. Perdrix, and R. Vilmart. Diagrammatic reasoning beyond Clifford+T quantum mechanics. In *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS '18, pages 569–578, New York, NY, USA, 2018. ACM.

[62] E. Jeandel, S. Perdrix, and R. Vilmart. A generic normal form for zx-diagrams and application to the rational angle completeness. *arXiv preprint arXiv:1805.05296*, 2018.

[63] E. Jeandel, S. Perdrix, R. Vilmart, and Q. Wang. Generalised supplementarity and new rule for empty diagrams to make the zx-calculus more expressive. *arXiv preprint arXiv:1702.01945*, 2017.

[64] E. Jeandel, S. Perdrix, R. Vilmart, and Q. Wang. ZX-calculus: Cyclotomic supplementarity and incompleteness for Clifford+T quantum mechanics. In K. G. Larsen, H. L. Bodlaender, and J.-F. Raskin, editors, *42nd International Symposium on Mathematical Foundations of Computer Science (MFCS 2017)*, volume 83 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages

11:1–11:13, Dagstuhl, Germany, 2017. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[65] R. Jozsa. An introduction to measurement based quantum computation. arXiv.org:quant-ph/0508124, 2005.

[66] D. Kartsaklis, M. Sadrzadeh, S. Pulman, and B. Coecke. Reasoning about meaning in natural language with compact closed categories and Frobenius algebras. *Logic and Algebraic Structures in Quantum Computing*, page 199, 2013.

[67] E. Kashefi, D. Markham, M. Mhalla, and S. Perdrix. Information flow in secret sharing protocols. *EPTCS 9, 2009, pp. 87-97*, 09 2009.

[68] A. Keet, B. Fortescue, D. Markham, and B. C. Sanders. Quantum secret sharing with qudit graph states. *Physical Review A*, 82:062315, 2010.

[69] A. Kotzig. Eulerian lines in finite 4-valent graphs and their transformations. In *Colloqium on Graph Theory*, pages 219–230. Academic Press, 1968.

[70] J. Kratochvil. Perfect codes in general graphs. In *7th Hungarian colloqium on combinatorics*, 1987.

[71] A. Marin, D. Markham, and S. Perdrix. Access structure in graphs in high dimension and application to secret sharing. In *8th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC'13) – to appear in LNCS*, 2013.

[72] D. Markham and B. C. Sanders. Graph states for quantum secret sharing. *Physical Review A*, 78:042309, 2008.

[73] D. Markham and B. C. Sanders. Graph states for quantum secret sharing. *Physical Review A*, 78:042309, 2008.

[74] K. Matsumoto and K. Amano. Representation of quantum circuits with Clifford and $\pi/8$ gates. June 2008.

[75] M. Mhalla and S. Perdrix. Finding optimal flows efficiently. In *the 35th International Colloquium on Automata, Languages and Programming (ICALP), LNCS*, volume 5125, pages 857–868, 2008.

[76] M. Mhalla and S. Perdrix. Graph states, pivot minor, and universality of (X,Z)-measurements. *International Journal of Unconventional Computing (IJUC)*, 2012.

[77] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[78] S. Perdrix and Q. Wang. Supplementarity is necessary for quantum diagram reasoning. In *41st International Symposium on Mathematical Foundations of*

Computer Science (MFCS 2016), volume 58 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 76:1–76:14, Krakow, Poland, Aug. 2016.

[79] R. Prevedel, P. Walther, F. Tiefenbacher, P. Bohi, R. Kaltenbaek, T. Jennewein, and A. Zeilinger. High-speed linear optics quantum computing using active feed-forward. *Nature*, 445(7123):65–69, Jan. 2007.

[80] R. Raussendorf and H. Briegel. A one-way quantum computer. *Physical Review Letters*, 86(22):5188–5191, 2001.

[81] R. Raussendorf and H. Briegel. Computational model underlying the one-way quantum computer. *Quantum Information and Computation*, 6:433, 2002.

[82] R. Raussendorf and H. J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86:5188–5191, 2001.

[83] M. Rossi, M. Huber, D. Bruß, and C. Macchiavello. Quantum hypergraph states. *New Journal of Physics*, 15(11):113022, 2013.

[84] D. Schlingemann and R. F. Werner. Quantum error-correcting codes associated with graphs. *Physical Review A*, 65, 2001.

[85] C. Schröder de Witt and V. Zamdzhiev. The ZX-calculus is incomplete for quantum mechanics. In *QPL 2014*, Electronic Proceedings in Theoretical Computer Science, pages 285–292, 2014.

[86] P. Selinger. Dagger compact closed categories and completely positive maps. *Electronic Notes in Theoretical Computer Science*, 170:139–163, mar 2007.

[87] P. Selinger. Generators and relations for n-qubit Clifford operators. *Logical Methods in Computer Science*, Volume 11, Issue 2, June 2015.

[88] P. Selinger and X. Bian. Relations for Clifford+T operators on two qubits. 2015.

[89] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[90] J. A. Telle. Complexity of domination-type problems in graphs. *Nordic Journal of Computing*, 1:157–171, 1994.

[91] M. Van den Nest, A. Miyake, W. Dür, and H. J. Briegel. Universal resources for measurement-based quantum computation. *Phys. Rev. Lett.*, 97:150504, Oct 2006.

[92] P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger. Experimental one-way quantum computing. *Nature*, 434(7030):169–176, Mar. 2005.

[93] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[94] A. Yao. Quantum circuit complexity. In *Proc. 34th IEEE Symposium on Foundation of Computer Science*, 1993.

english

Annexe A

Introduction à l'informatique quantique

Nous proposons ici une brève introduction à l'informatique quantique. Cette section a été élaborée à partir de différentes notes de cours que j'ai constituées lors de mes différentes interventions d'introduction à l'informatique quantique (cours niveau master, cours en école jeunes chercheurs, présentations, etc.). Mes notes de cours, issues d'un cours de l'école des jeunes chercheurs en informatique mathématique 2016, ont été publiées [5].

A.1 Les postulats de la mécanique quantique

La formalisation de la mécanique quantique date du début du siècle passé. Même si de nombreuses questions fondamentales continuent à animer la communauté scientifique travaillant sur les fondements de la physique quantique (unification de la mécanique quantique et relativité générale, ou interprétation de la mesure quantique par exemple), le formalisme de la mécanique quantique est particulièrement solide et éprouvé : elle est la théorie physique la plus fidèle à la réalité dans le sens où cette théorie permet de prédire les résultats expérimentaux avec très grande précision.

Dans cette section, nous allons adopter une présentation de la mécanique quantique adaptée aux informaticiens : nous considèrerons uniquement des systèmes discrets et finis, où la brique de base de l'information est le bit quantique, ou *qubit*. Après avoir décrit les états possibles d'une mémoire quantique, nous verrons comment la mesure agit sur l'état d'un registre, et enfin nous verrons comment évolue l'état d'un système quantique isolé.

A.1.1 États Quantiques

Le bit quantique La brique de base en théorie de l'information est le *bit*. La mécanique quantique nous enseigne qu'un tel système ayant deux états classiques possibles **0** et **1** peut également être dans une superposition de **0** et de **1**, c'est-à-dire dans un état que nous noterons $\alpha\,|\mathbf{0}\rangle + \beta\,|\mathbf{1}\rangle$ où $\alpha, \beta \in \mathbb{C}$ avec $|\alpha|^2 + |\beta|^2 = 1$. De façon plus abstraite, l'espace des états possibles d'un bit quantique (*qubit*) est donc la sphère unité de $\mathbb{C}^{\{\mathbf{0},\mathbf{1}\}}$, le $\mathbb{C}$-espace vectoriel de dimension 2 engendré par $|\mathbf{0}\rangle$ et $|\mathbf{1}\rangle$ et muni de la norme euclidienne.

Plus généralement l'état d'un registre de n bits quantiques est une superposition des 2^n états classiques possibles :

Définition A.1.1. *L'état $|\varphi\rangle$ d'un registre quantique de taille n est un vecteur unité de $\mathbb{C}^{\{\mathbf{0},\mathbf{1}\}^n}$:*

$$|\varphi\rangle = \sum_{x\in\{\mathbf{0},\mathbf{1}\}^n} \alpha_x\,|x\rangle \quad \textit{tel que} \quad \|\,|\varphi\rangle\,\| = \sqrt{\sum_{x\in\{\mathbf{0},\mathbf{1}\}^n} |\alpha_x|^2} = 1$$

Exemple A.1.2.

$$\frac{1}{\sqrt{2}}(|00\rangle - |01\rangle)$$

$$\frac{1}{\sqrt{3}}(|00\rangle + i\,|01\rangle + |11\rangle)$$

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

Remarque A.1.3 (Notation de Dirac)**.** *Le symbole $|x\rangle$ se prononce 'ket' x. On utilise également le symbole $\langle x|$ qui se prononce 'bra' x pour parler de l'adjoint $|x\rangle^\dagger$ de $|x\rangle$. Les termes 'bra' et 'ket' proviennent de la décomposition du mot 'bracket' utilisé pour parler du produit scalaire canonique $\langle u|v\rangle = u^\dagger v$, ainsi le produit de $\langle x|$ ('bra') et $|y\rangle$ ('ket') est le produit scalaire ('bracket') des deux vecteurs, i.e. $\langle x|y\rangle = \langle x|\,|y\rangle$.*

Système composé

L'état d'un registre classique dont on connait l'état des sous-registres est obtenu par simple concaténation de ces états : par exemple un registre de 3 bits dont les deux premiers sont dans l'état **01** et le troisième est dans l'état **1**, est dans l'état **011**. La composition des états quantiques s'obtient à l'aide du produit tensoriel :

Définition A.1.4. *Soit $|\varphi_1\rangle$ l'état d'un registre de n qubits et $|\varphi_2\rangle$ celui d'un registre de m qubits, l'état du registre composé de $(n+m)$ qubits est*

$$|\varphi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle$$

avec $\cdot\otimes\cdot$ bilinéaire et $\forall x \in \{\mathbf{0},\mathbf{1}\}^n, \forall y \in \{\mathbf{0},\mathbf{1}\}^m, |x\rangle \otimes |y\rangle = |xy\rangle$

L'état d'un registre composé d'un premier sous registre dans l'état $\sum_{x\in\{\mathbf{0},\mathbf{1}\}^n} \alpha_x |x\rangle$ et d'un second dans l'état $\sum_{y\in\{\mathbf{0},\mathbf{1}\}^m} \beta_y |y\rangle$ est donc $\sum_{x\in\{\mathbf{0},\mathbf{1}\}^n, y\in\{\mathbf{0},\mathbf{1}\}^m} \alpha_x\beta_y |xy\rangle$.

Exemple A.1.5. *Dans les exemples qui suivent nous utilisons deux couleurs dans un but pédagogique pour mettre en évidence le premier registre (en bleu) et le second (en rouge).*

$|\mathbf{0}\rangle \otimes \frac{|\mathbf{0}\rangle-|\mathbf{1}\rangle}{\sqrt{2}} = \frac{|\mathbf{0}\rangle\otimes|\mathbf{0}\rangle-|\mathbf{0}\rangle\otimes|\mathbf{1}\rangle}{\sqrt{2}} = \frac{|\mathbf{00}\rangle-|\mathbf{01}\rangle}{\sqrt{2}}$

$\frac{|\mathbf{0}\rangle+i|\mathbf{1}\rangle}{\sqrt{2}} \otimes \frac{|\mathbf{00}\rangle-i|\mathbf{10}\rangle}{\sqrt{2}} = \frac{|\mathbf{000}\rangle-i|\mathbf{010}\rangle+i|\mathbf{100}\rangle+|\mathbf{110}\rangle}{2}$

L'état d'un registre sur plusieurs qubits n'est pas toujours décomposable en l'état de chacun de ses qubits. Par exemple pour tous $|\varphi_1\rangle$, $|\varphi_2\rangle$ états quantiques sur un qubit, $|\varphi_1\rangle \otimes |\varphi_2\rangle \neq \frac{1}{\sqrt{2}}(|\mathbf{00}\rangle + |\mathbf{11}\rangle)$. En effet, soient $|\varphi_1\rangle = a|\mathbf{0}\rangle + b|\mathbf{1}\rangle$ et $|\varphi_2\rangle = c|\mathbf{0}\rangle + d|\mathbf{1}\rangle$, on a $|\varphi_1\rangle\otimes|\varphi_2\rangle = ac|\mathbf{00}\rangle + ad|\mathbf{01}\rangle + bc|\mathbf{10}\rangle + cd|\mathbf{11}\rangle$. Comme le système $\{ac = 1/\sqrt{2}; ad = 0; bc = 0; cd = 1/\sqrt{2}\}$ n'a pas de solution, l'état $\frac{1}{\sqrt{2}}(|\mathbf{00}\rangle + |\mathbf{11}\rangle)$ est indécomposable, on dit qu'il est *intriqué*. La découverte mathématique de tels états par Einstein, Podolsky et Rosen [43] en 1935 les a conduit à remettre en cause le formalisme de la mécanique quantique. Dans les années 60, John Bell [12] a proposé une expérience permettant de décider si de tels états existent ou non dans la nature. Malheureusement cette expérience était irréalisable avec les technologies de l'époque. En 1982, Alain Aspect et son équipe [6] réalisent l'expérience de Bell et démontrent expérimentalement l'existence de tels états quantiques intriqués.

L'intrication est un phénomène essentiel en informatique quantique : elle est utilisée dans le protocole de téléportation par exemple. Elle est également indispensable au calcul quantique : un ordinateur quantique dont la mémoire serait à tout moment séparable (c'est-à-dire sans intrication) peut être simulé efficacement par un ordinateur classique.

États graphes

Représenter et manipuler un état quantique n'est pas toujours aisé : un état quantique sur n qubits est représenté par 2^n nombres complexes. Concrètement, la description d'un état sur 20 qubits peut nécessiter jusqu'à plus d'un million de nombres complexes. Certains états quantiques admettent cependant une représentation plus compacte, c'est le cas des états graphes [53]. Les états graphes sont des états quantiques représentés par des graphes simples non orientés où chaque sommet correspond à un qubit et chaque arête représente intuitivement l'intrication entre les qubits. Formellement, étant donné un graphe $G = (V, E)$ d'ordre $n = |V|$, l'état quantique $|G\rangle$ représenté par ce graphe est

$$|G\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{\mathbf{0},\mathbf{1}\}^V} (-1)^{|G[x]|} |x\rangle$$

où $|G[x]|$ est la taille du sous graphe induit par le support de x, autrement dit $|G[x||$ est le nombre d'arêtes (u, v) de G telles que $x_u = x_v = 1$.

A.1.2 Mesure quantique

La mécanique quantique nous dit que si un système peut être dans deux états – par exemple un bit dans l'état 0 ou 1 ; ou un chat vivant ou mort – alors ce système peut être dans une superposition de ces deux états. Or, dans la vie de tous les jours nous observons rarement des superpositions de 0 et de 1 et encore moins des chats à la fois vivants et morts ! Une explication à cela : l'observation, aussi appelée mesure quantique, obéit à un postulat qui ne rend que les états *classiques* directement obervables. Si un qubit dans l'état $\alpha |\mathbf{0}\rangle + \beta |\mathbf{1}\rangle$ est mesuré alors avec probabilité $|\alpha|^2$ la valeur $\mathbf{0}$ est observée et avec probabilité $|\beta|^2$ la valeur $\mathbf{1}$ est observée. De plus, la mesure projette l'état du qubit dans l'état observé, à savoir $|\mathbf{0}\rangle$ dans le premier cas et $|\mathbf{1}\rangle$ dans le second.

$$\alpha |\mathbf{0}\rangle + \beta |\mathbf{1}\rangle \xrightarrow{|\alpha|^2} |\mathbf{0}\rangle \text{ on mesure } \mathbf{0}$$
$$\alpha |\mathbf{0}\rangle + \beta |\mathbf{1}\rangle \xrightarrow{|\beta|^2} |\mathbf{1}\rangle \text{ on mesure } \mathbf{1}$$

Dans le cas des états intriqués, la mesure d'un qubit modifie globalement l'état du système : par exemple si le premier qubit de l'état $\frac{|\mathbf{00}\rangle + |\mathbf{11}\rangle}{\sqrt{2}}$ est mesuré, avec probabilité 1/2 le premier qubit sera projeté dans l'état $|\mathbf{0}\rangle$ (resp. $|\mathbf{1}\rangle$) et donc l'état global du système sera $|\mathbf{00}\rangle$ (resp. $|\mathbf{11}\rangle$). Ainsi l'état du second qubit dépend du résultat de la mesure du premier qubit. Il y a ici un effet de bord instantané de la mesure du premier qubit sur le second et ce quelque soit la distance physique entre ces deux qubits. Bien qu'ayant contribué au scepticisme face à l'existence des états intriqués, cette non localité de la mesure quantique ne viole pas le principe de causalité car elle ne permet pas de transmettre d'information plus vite que la vitesse de la lumière. La raison est essentiellement que le résultat de la mesure est probabiliste, on ne peut donc pas 'choisir' de projeter l'état du second qubit dans un état ou dans un autre.

La définition suivante décrit l'action de la mesure d'un des qubits d'un registre quantique :

Définition A.1.6. *La mesure du $i^{ième}$ qubit de $\sum_{x\in\{\mathbf{0},\mathbf{1}\}^n} \alpha_x |x\rangle$ produit le résultat $r \in \{0, 1\}$ avec probabilité $p_r = \sum_{x\in\{\mathbf{0},\mathbf{1}\}^n \mid x_i=r} |\alpha_x|^2$, l'état du registre après la*

mesure[1] *est alors* $\frac{1}{\sqrt{p_r}} \sum_{x \in \{\mathbf{0},\mathbf{1}\}^n \mid x_i = r} \alpha_x |x\rangle$.

On peut donc voir la mesure du $i^{\text{ième}}$ qubit comme la transition probabiliste suivante :

$$\sum_{x \in \{\mathbf{0},\mathbf{1}\}^n} \alpha_x |x\rangle \quad \xrightarrow[p_r]{} \quad \frac{1}{\sqrt{p_r}} \sum_{x \in \{\mathbf{0},\mathbf{1}\}^n \mid x_i = r} \alpha_x |x\rangle$$

La mesure décrite ci-dessus est une mesure dans la base dite *standard* $\{|\mathbf{0}\rangle, |\mathbf{1}\rangle\}$. Plus généralement, on peut faire des mesures dans toute base $\{|\psi_0\rangle, |\psi_1\rangle\}$ orthonomée ($\langle\psi_0|\,|\psi_1\rangle = 0$, où $\langle\psi_0| := |\psi_0\rangle^\dagger$). D'un point de vue physique, mesurer dans une autre base signifie mesurer une autre quantité : mesurer l'énergie ou la position d'une particule correspond à des mesures dans des bases différentes.

A.1.3 Évolution unitaire, isométries

En l'absence de mesure, c'est à dire quand le système est isolé, l'évolution quantique est une isométrie : son évolution est linéaire et préserve la condition de normalisation.

Définition A.1.7. *L'évolution d'un système isolé est une isométrie.* $U : \mathbb{C}^{\{\mathbf{0},\mathbf{1}\}^n} \to \mathbb{C}^{\{\mathbf{0},\mathbf{1}\}^m}$ *est une isométrie si*

— U *est linéaire :* $U(\alpha |\phi\rangle + \beta |\psi\rangle) = \alpha U |\phi\rangle + \beta U |\psi\rangle$;

— U *préserve la norme euclidienne :* $\|U |\phi\rangle\| = \||\phi\rangle\|$.

Une isométrie est une opération inversible :

Propriété A.1.8. $U : \mathbb{C}^{\{\mathbf{0},\mathbf{1}\}^n} \to \mathbb{C}^{\{\mathbf{0},\mathbf{1}\}^m}$ *est une isométrie si et seulement si* $U^\dagger = U^{-1}$ *où* $U^\dagger$ *est l'adjoint – c'est à dire la transposée conjuguée – de* U.

Une évolution unitaire est une isométrie dont le domaine et co-domaine sont de même dimension. À noter que si $U : \mathbb{C}^{\{\mathbf{0},\mathbf{1}\}^n} \to \mathbb{C}^{\{\mathbf{0},\mathbf{1}\}^n}$ est unitaire alors son inverse $U^\dagger$ est également unitaire (ce qui est faux pour une isométrie non-unitaire). Toute isométrie peut être vue comme une transformation unitaire agissant sur des qubits auxiliaires initialisés dans l'état $|0\rangle$:

Propriété A.1.9. *Pour tout isométrie* $V : \mathbb{C}^{\{\mathbf{0},\mathbf{1}\}^n} \to \mathbb{C}^{\{\mathbf{0},\mathbf{1}\}^m}$, *il existe une transformation unitaire* $U : \mathbb{C}^{\{\mathbf{0},\mathbf{1}\}^m} \to \mathbb{C}^{\{\mathbf{0},\mathbf{1}\}^m}$ *telle que pour* $|\phi\rangle \in \{0,1\}^n$, $V(|\phi\rangle) = U(|\phi\rangle \otimes |0^{m-n}\rangle)$.

1. Lorsque $p_r = 0$ l'état du registre après la mesure n'est pas défini (division par 0), mais la mesure ne produit, par définition, jamais ce cas là.

Exemple A.1.10. *Les opérations unitaires sur* 1 *qubit les plus simples sont les opérations de Pauli* X, Y, Z *:*

$$X : \begin{matrix} |0\rangle & \mapsto & |1\rangle \\ |1\rangle & \mapsto & |0\rangle \end{matrix} \qquad Z : \begin{matrix} |0\rangle & \mapsto & |0\rangle \\ |1\rangle & \mapsto & -|1\rangle \end{matrix} \qquad Y = iXZ : \begin{matrix} |0\rangle & \mapsto & i|1\rangle \\ |1\rangle & \mapsto & -i|0\rangle \end{matrix}$$

En notation de Dirac : $X = |1\rangle\langle 0| + |1\rangle\langle 0| = \sum_{x\in\{0,1\}} |1-x\rangle\langle x|$, $Z = \sum_{x\in\{0,1\}} (-1)^x |x\rangle\langle x|$, *et* $Y = i\sum_{x\in\{0,1\}} (-1)^x |x\rangle\langle x|$.
D'autres exemples sont la transformation d'Hadamard (H*) et une extension de Pauli* Z *appelé rotation autour de* Z *:*

$$H = \frac{1}{\sqrt{2}} \sum_{x,y\in\{0,1\}} (1)^{xy} |x\rangle\langle y| \qquad R_z(\theta) = \sum_{x\in\{0,1\}} e^{ix\theta} |x\rangle\langle x|$$

Le Control-Not (ΛX*) est une transformation unitaire agissant sur* 2 *qubits. Intuitivement une négation (Pauli* X*) est appliquée sur le second qubit si le premier est dans l'état* $|1\rangle$ *:*

$$\Lambda X : \begin{matrix} |00\rangle & \mapsto & |00\rangle \\ |01\rangle & \mapsto & |01\rangle \\ |10\rangle & \mapsto & |11\rangle \\ |11\rangle & \mapsto & |10\rangle \end{matrix}$$

De façon plus compacte, $\Lambda X = \sum_{x,y\in\{0,1\}} |x, y \oplus x\rangle\langle x, y|$.

La transformation d'Hadamard est particulièrement utile en informatique quantique car elle permet de produire des états superposés à partir d'états de bases (états classiques). Si l'on applique Hadamard une seconde fois,

$$HH|0\rangle = H\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{H|0\rangle + H|1\rangle}{\sqrt{2}} = \frac{|0\rangle + |1\rangle + |0\rangle - |1\rangle}{2} = |0\rangle$$

on voit apparaitre un autre phénomène spécifiquement quantique, l'interférence entre $+|1\rangle$ et $-|1\rangle$, pour obtenir l'état classique $|0\rangle$.

La composition spaciale de transformations unitaires est obtenue grâce au produit tensoriel :

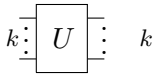
Définition A.1.11. *Soient* U *l'évolution unitaire d'un registre de* n *qubits et* V *celle d'un registre de* m *qubits, l'évolution globale du registre composé de* $(n+m)$ *qubits est* $U \otimes V$ *avec* $\forall x \in \{\mathbf{0},\mathbf{1}\}^n, \forall y \in \{\mathbf{0},\mathbf{1}\}^m, (U \otimes V)|x, y\rangle = (U|x\rangle) \otimes (V|y\rangle)$.

A.2 Circuits quantiques

Les portes d'un circuit quantique sont des transformations unitaires. Tout circuit quantique est réversible, il possède autant d'entrées que de sorties. Étant donnée

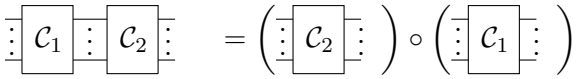
une famille $\mathcal{F}$ de transformations unitaires, un circuit quantique peut être défini inductivement de la façon suivante :

— Porte $U \in \mathcal{F}$ d'arité k :

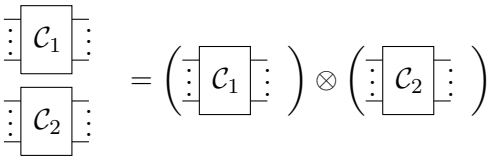


— L'identité :

— Composition séquentielle de deux circuits $\mathcal{C}_1$ et $\mathcal{C}_2$, agissant tous deux sur n qubits :



— Composition parallèle de deux circuits $\mathcal{C}_1$ et $\mathcal{C}_2$:



Le nombre de portes d'un circuit est appelé sa taille.

Théorème A.2.1 ([77]). *La famille de portes unitaires* $\{H, \Lambda X, R_z(\alpha) : \alpha \in [0, 2\pi[\}$ *est universelle : pour tout* n*, et pour toute transformation unitaire* U *sur* n *qubits, il existe un circuit quantique réalisant* U *dont chaque porte est* H*,* ΛX *ou* $R_z(\alpha)$*.*

La famille $\{H, \Lambda X, R_z(\alpha) : \alpha \in [0, 2\pi[\}$ est universelle mais infinie non dénombrable. Il n'est pas très raisonnable de définir un modèle de calcul en autorisant des angles qui ne sont pas calculables, de plus en pratique aucune technologie ne permet d'implémenter une rotation selon un angle fixé α_0 avec une infinie précision.

La sous-famille $\{H, \Lambda X, Z\}$ est appelée opérations de Clifford. Les opérations de Clifford forment une famille interessante d'opérations quantiques, on peut par exemple créer des états graphes, ou réaliser des protocoles quantiques comme la téléportation [14], le super-dense coding [15] ou encore la distribution quantique de clés BB84 [13] dans en utilisant des opérations de Clifford. Ce fragment n'est cependant pas universel. Pire, tout algorithme quantique pouvant être décrit dans ce fragment peut être simulé efficacement avec un ordinateur classique.

En revanche, en ajoutant simplement $T = R_Z(\pi/4)$ aux opérations de Clifford (fragment appelé logiquement Clifford+T) on obtient un fragment certes non universel (le nombre de circuits possibles est dans ce cas dénombrable alors que l'ensemble des opérations unitaires sur n qubits, pour $n > 0$ fixé, ne l'est pas), mais approximativement universel ;

Théorème A.2.2 ([77]). *La famille Clifford+T des portes unitaires* $\{H, \Lambda X, R_z(\pi/4)\}$ *est approximativement universelle : pour tout* n*, pour tout transformation unitaire* U *sur* n *qubits et pour toute* $\epsilon > 0$*, il existe un circuit quantique réalisant une transformation unitaire* U_0 *telle que* $\|U - U_0\| < \epsilon$*, où* $\|V\| = \sup_{|\phi\rangle \neq 0} \frac{\||V|\phi\rangle\|}{\||\phi\rangle\|}$.